A User's Guide To The Dark Web

The 42nd and Final Encyclopedia Cyberspacia

By Lefty Insider (arister0s n0stis)

Encyclopedia Cyberspacia

Target Market

This Guide is intended as a companion to my novel The Insider Goes Deep.

I want you, to go deep?

Acknowledgements
Those involved in the creation of this book, know who they are.

Editor and publisher
Last edited November 2022

ISBN number

U.S. Copyright Office
Copyright 1-4315250291
Case Date: 1/6/2017

Apart from the well-known actual people, events, and locales that figure into the narrative, all names, characters, places, and incidents are products of the writer's imagination or are used fictitiously.

Synopsis

A how-to book on how to safely navigate and survive the Dark Web. Appendices include information regarding online history, philosophy, anonymity, and privacy in general.

Book Four
A User Guide To The Dark Web
(The 42nd and Final Encyclopedia Cyberspacia)
Approximately 88k words, 400 pages TBD
Approximately 30 footnotes, 300 illustrations
Approximately 400 CW links and 200 DW links
Approximately 40 Notes

The above is a companion book to:

Book Three

- *The Insider Goes Deep (Tales from the Dark Web)*
  Approximately 90k words, 400 pages TBD
  Approximately 50 footnotes, 200 illustrations
  Approximately 200 CW links and 50 DW links
  Approximately 30 Notes

This book is a supplement to, or extension of, my third book and the finale in the Insider trilogy, which collectively encompass a 50-year period modern day Bildungsroman for the Lefty character and his life lived largely mediated by computer screens.

This is fourth book is intended to be a reference book and an addition to the Library of Imperial Trantor on the Dark Web.

The Dark Web in reality consists of websites that exist in darkness, on overlay networks that use the Internet but require specific software, configurations, or authorization to access.

This guide exposes what you need to do and what you need to know to successfully transition through the Dark Web of semi-private computer networks. This part of Cyberspacia is where individuals can communicate and conduct business anonymously without divulging identifying information, such as personal identification or a user's location. The Dark Web consists of small, friend-to-friend peer-to-peer networks, as well as large, popular networks such as Tor, Freenet, I2P, and Riffle operated by semi-public organizations and individuals.

This book seeks to answer the following questions, while educating the reader with helpful information.

The Dark Web (Net)

What is it?
Where is it?
How does it work?
How do you use it?
Who is there?
What are they doing?
Why are they doing it?

TeachPrivacy
Why are you going on the Dark Web?
I forgot my password so I need to look it up.
DARK WEB
Welcome!
And have a great day!
Written by Daniel J. Solove
www.teachprivacy.com
Illustrated by Ryan Beckwith

Are your passwords on a Post-it under your keyboard?

A note to readers:

Throughout this book and the three previous prequels, this writer has chosen to write the term Internet with its original initial capitalization spelling as a proper noun. The Internet is a person, place, or thing and as we were all taught in grade school, and as such it requires proper capitalization. The current trend in print and online spelling as *lower case* I believe to be grammatically wrong as well as disrespectful to its founders and creators.

I also believe that this current revision is an intentional diminishment, via the lower case spelling of this technological wonder and gift to humanity, is part of an effort by Corporate America to assimilate it into their Corporate Borg. To the founders, decentralization was the main idea; it was not the current walled gardens of Google, Apple, Amazon, Microsoft, and Facebook (META). While original pioneers like Vint Cerf may have been assimilated into the corporate Borg, people like Jon Postel and Tim Berners-Lee never were. Anyway, as the writer here, widely published or not, I get to decide things like this.

Non-original text formatting conventions

Text coming from "Websites" will be formatted thus.

Text coming from "Wikipedia" will be formatted thus.

Text coming from "News" sources will be formatted thus.

For purposes of clarity and the safety of your privacy, the following conventions of symbols are used throughout this book to identify web page links (hyperlinks) as either:

Clear Web (std. Clear Web browser (.com, .org. .gov, .io, .net, country domain, etc.)

Dark Web (Tor) (.onion)

This will ensure that you know exactly where you are going on the Internet and what trail you are leaving behind.

Note: this book is best read with a pdf reader, in Read Mode, and in portrait orientation, which allows for page turning and also to zoom in on the graphics. 1600x900 or higher screen resolution is recommended.

Note: any hyphens visible in the URL's are for text formatting purposes only. These hyperlinks will function from this pdf if clicked on and as a result should not be copied and pasted into a web browser.

Foreword

This Guide is intended to provide you the information required to efficiently and safely navigate the Dark Web.

Following the chapters, you will find appendices, which provide supplemental information, history, and opinion about Cyberspace.

Fair use rationale for illustrations & lyrics

This publication does not limit, nor claim to limit, the rights of the copyright holder. They remain the property and copyright of their owners.

Partial song lyrics are used as descriptive words.

Other graphics are either self-created, public domain via Wikimedia Commons, where attribution is not required, or come from the Creative Commons.

Images used are copyleft, screen shots, creative commons, Wikipedia or in the public domain. i.e.

https://www.pexels.com/search/darkweb/

Copyright disclaimer under Section 107 of the Copyright Act of 1976, allowances are made for "Fair Use" for purposes such as criticism, comment, news reporting, teaching, scholarship, and research. Fair Use is a use permitted by copyright statute that might otherwise be infringing. Non-Profit, educational, or personal use tips the balance in favor of Fair Use.

This guide is an open-source non-profit initiative, licensed under Creative Commons Attribution-Noncommercial 4.0 International (cc-by-nc-4.0 [Archive.org]) and is not sponsored/endorsed by any commercial/governmental entity. This means that you are free to use this guide for any purpose excluding commercially as long as you attribute it.

Table of Contents

Contents

Target Market 1
Synopsis 2
A note to readers: 4
Foreword 5
Fair use rationale for illustrations & lyrics 6
Table of Contents 7
Introduction 15
Navigating the Dark Web 24

When was the Dark Web invented? 24
How deep is the Deep Web? 25
Are there bad things on the Dark Web? 26

Keystroke Logging and Keyloggers 28
Anti-keylogger Software 28
Botnets 28
Onion Links 29

A Short History of Tor 30

Tor Bridges 34
TorStatus - Connection stats. 36
Map of all Tor Relays 36
Dark Web.wtf 46
The best links to Tor browser v3 2021 46
Http:\\ or Https:\\ on onion sites? 47
Tor Tools 50
Learn more about Tor 50

What Not To Do While Using TOR 51
Tor Identities 54
How to verify an Onion 55
Do Look at your Tor Logs 57
Being Safe on the Dark Web 59
Browser Fingerprinting 61

To Dark Web Search 67

Search Sites 68

Ahmia 68
HiddenWiki 69
OnionLinks 69

Duckduckgo 70
Why is the Deep Web not indexable? 72
Onion Search Engine 77
TorDex 77
Pick your search engine in Tor 78
HayStak 79
Recon Search Site 79
Deeplink Onion Directory 80
Clear Web crawlers (spiderbots) 81
Dark Web crawlers (spiderbots) 82
Dark Web Forums 84
Typical DW Forum Rules (they have rules?) 87
DarknetHub 89
The Majestic Garden 90
Breaking Bad 91
Incognito Market 92
Raddle 96
So not really the Dark Web here, and deeper down the rabbit hole we will now go. 97
The Hub 98
Envoy 113
dread 117
Dark Web Email 144
TorBox Email 144
ProtonMail 145
Mail2Tor - Anonymous Email Service Provider 146
Elude 147
List of email providers 148
Tutanota 149
Secmail 149
Secmail.Pro 150
Juvenile - No Rules 151
Top 5 Dark Web Email Providers (another list) 154
ProtonMail.com 154
TorBox 156
Bitmessage 156
Mail2Tor 157
Cock.li 158
Others 158

Conclusion 160
Dark Web Onion News Sites 161
ProPublica 161
Darknetlive 161
FlashLight Deep Web News 162
The Intercept 162
Dark Web Link 162
Chat Rooms 163
Paradise 163
element 164
Endchan 165
2chan, 4chan, 8chan, oh my! 166
8chan.moe 169
Jitsi 170
Social Media 171
The Jabber network 171
Chat 176
Dark Web Monitoring 177
DNstats 177
Surveilled 178
ShieldsUp 179
What's DNS poisoning, anyway? 179
Why collect it all? 184
Other Resources 185
Data Brokers 186
Why is this a problem? 186
What can you do about it? 187
Data Breaches 189
Data Breaches 190
Who Was Involved In The NSA Hack? 191
Ransomware 192
Malware 196
Microsoft Security Essentials 196
ESET 197
Managing attachments with Dangerzone 198
URL defanging 198

Operating Systems 199
Tails/Whonix/Qubes 199
Other Linux distros (but not all 270) 205
How to prepare Windows 7 Ultimate 64 bit for the Internet in general and also the DW 211
Windows 10/11…do not despair as they are not completely hopeless but do not use on the DW 214
More about software 217
VPN's 219
When to use a VPN? 219
Encryption and PGP 224
OpenPGP 228
GnuPG 234
Canary 235
Warrant Canary 236
Dark Web Tor Hosting 238
Finding an ISP to host a DarkNet .onion site 239
DeepLink Onion Directory 239
Types of Server Hosting: 240
Dedicated 240
VPS 240
RDP Service Hosting 240
What is a Tor Exit Node 241
What is the difference between the Single Hop Onions and MultiHop Onion Options? 241
So are Multi Hop Onions Anonymous? 241
Dark Web Server Hosting 242
Perfect Quality Hosting 242
AlexHost 242
CryptoHOST 242
VPSBG 242
Evolution Host 243
sthosting 243
BuyVM 243
KoDDoS 243
IQ.PL 243
Privex 244
Portlane 244

UDN (Ukrainian Data Network) 244
Psychz Networks 244
netcup 245
TrilightZone 245
Ablative Hosting 245
AnyCOLO.Net 246
Swiss Layer 246
EPIO.HOST 246
5WIRE 246
Userbase 247
NiceVPS.net 247
Cryptwerk 247
Monero VPS 247
ABACOHosting 247
QHoster 247
What The Server 248
Codify 248
Super Byte Hosting, ... 248
SuperbitHOST 248
Nexwave 248
HOSTINTSSi 248
BlazinHosting 248
Laweitech Company Limited 248
1984 249
snel.com 249
Njalla 249
BaCloud 249
CryptoFibers 249
Sporestack 250
99Stack 250
Rad Web Hosting 250
PacketPoint 250
Server Where (SW) 250
Host Havoc 251
Coinhost.io 251
1Gbits 251
bithost 251
AirVPN 251
Builderra 251
IMPREZA 251
ipxcore 252
orangewebsite. 252
COIN.HOST 252

EndGame 253
Whistleblowing / Drop sites 254
SecureDrop 254
Distributed Denial of Secrets 254
File uploads and transfers 255
File transfer (secure FTP or SFTP) 256
Anonfiles 257
Tor Alternatives 258
More than Tor 258
Tor alternative #1: I2P 259
Tor alternative #2: Tails 260
Tor alternative #3: Subgraph OS 262
Tor alternative #4: Freenet 262
Tor alternative #5: Freepto 263
Other Alternatives 264
Alternate Sites 270
Imperial Library of Trantor 270
Just Another Library 272
Libraries A more complete list. 272
Deep Web Radio 273
Onionland's Museum 273
File Sharing 273
CryptBB 273
Dark Web OpSec 275
KickAss 275
Dread 275
Verify your safety with Dark Fail's new PGP Tool 280
Surveillance Self-Defense 280
Global surveillance 280
The Matrix 281
How to Exit the Matrix 281
Web 3.0 (Web3) 282
Enter The Web3 Foundation 285
Bitcoin and the Block Chain 287
What the Heck is a Bitcoin? 287
What the Heck is a Blockchain? 290
Smart Contracts 294

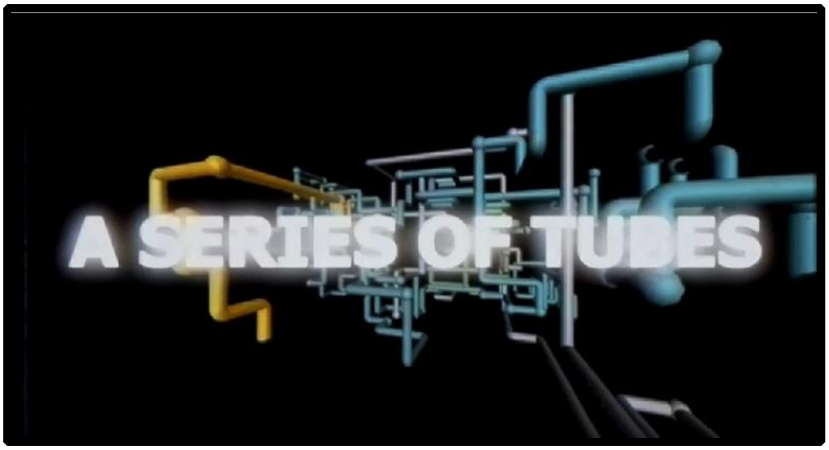
Artificial Intelligence (AI) 295
Metaverse 296
The Cloud 297
Botched and silent patches from Microsoft put customers at risk, critics say 297
Alternate hypertext or Web interfaces 298
Yandex browser 298
Vivaldi 300
Sleipnir 301
SRWareIron 302
Epic 303
Maxthon 305
Neil Young Archives 306
Project Xanadu 307
IOT (The Internet of Things) 309
Appendices 312
Have I Been Pwned? 313
Encrypting Outlook email on the Clear Web 314
The Basics of Hacking 315
Are you leaking IP and ID info? 318
IP Leaks 318
DNS Leaks 318
WebRTC IP Leak 319
Windows Privacy Dashboard 319
Windows Spy Blocker 320
Netstat 363
Ping 363
Wireshark 363
Think your Data is Safe in the Cloud? 365
NSA NETWORK INFRASTRUCTURE SECURITY GUIDANCE 371
What data Facebook (Meta) collects 372
Stop using Google 383
Stop Using Amazon 386
Broadband Internet for All 388
Free the Internet 392
A Clear and Transparent Digital Bill of Rights 396
The Hacker Manifesto 398
A Cypherpunks Manifesto 400
The Crypto Anarchist Manifesto 403

THE CYPHERNOMICON 405
A Declaration of the Independence of Cyberspace 407
Guerilla Open Access Manifesto 410
Contract-for-the-Web 412
Declaration-for-the-Future-for-the-Internet 414
The 10 Biggest Revelations From Edward Snowden's Leaks 420
8 Things That Happened Because Of The NSA Leaks 422
Whistleblowing Is Not Just Leaking — It's an Act of Political Resistance 425
Rear cover 432

Introduction

The World Wide Web also called the Surface Web or Clear Web (mostly encrypted[1], thus sometimes clear), is a *part* of the Internet. It is not as some think that the Web is THE Internet nor is Facebook, Google, Apple, Amazon, and Microsoft. They are just parts of the whole. It is now more than a billion websites that a typical search engine used now by more than three billion worldwide users. You access it with a web browser such as Microsoft Internet Explorer, Microsoft Edge, Google Chrome, Safari, Pale Moon, Brave, or better yet Mozilla Firefox.

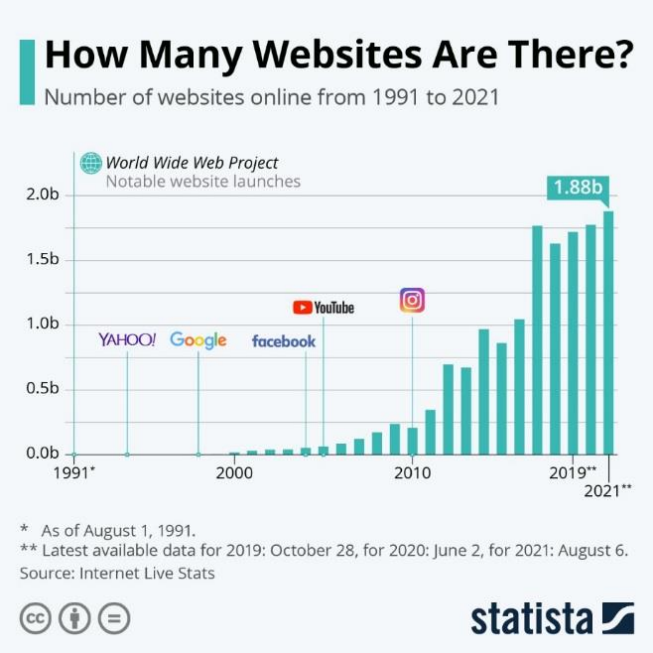
What the Internet in general is not is:



Although some of the unenlightened have been known to call it this.

[1] *Encoded to prevent easy viewing.*

The Deep Web (we are talking about Deep not Dark here) is also a part of the Internet and consists of anything that a standard search engine cannot access outside the enormous one billion; some estimates are as high as four billion, or so websites existing on servers around the globe. Spiders or also called bots crawl the surface web to populate the search engine databases but cannot effectively reach into the Deep Web.



Deep Web content can be found almost anytime you navigate away from a typical search engine and do a search directly in a website – government databases and libraries contain huge amounts of Deep Web data. Searching the archives of a newspaper is an example of the Deep Web. It can also mean that router settings have deliberately or accidentally have made accessing these hosts virtually impossible. Some estimates put this part of the Internet at 400 to 500 times larger than the Surface Web.

For example if you navigate to www.ssa.gov and login, it will take you to https://secure.ssa.gov/mySSA/start. This is a secure https[2] site in Deep Web.

[2] *Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP) for secure encrypted communication over a computer network.*

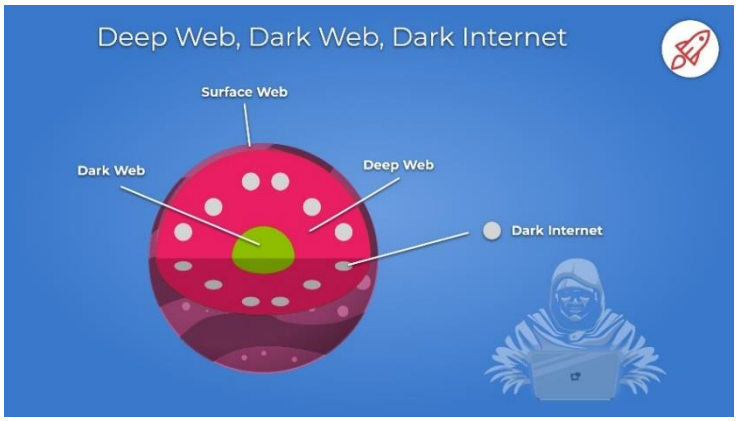
What the Deep Web consists of are some of the things you cannot find on the Surface Web.

- Password protected pages.
- Attendance records, Medical certificates etc.
- Bank records.
- Encrypted Chat Messages (WhatsApp, Facebook Messenger etc.)
- E-mails sent between users.
- Purchase-requiring content when not indexed on Search Engines (songs/ videos, school courses, etc.).

So in a nutshell, the content, which exists on the Internet, but cannot be accessed via Search Engines, or requires special permission, is Deep Web content.

Some websites also intentionally "de-index" themselves, so that they can only be accessed by people who know the exact URLs, these websites are also a part of the Deep Web, and host thing such as harmless discussions on conspiracy theories, and other such stuff.

Some refer to this as The Dark Internet and is similar to the Dark Web but actually is web data that is specific to one particular niche that users want to keep private. This is usually raw data used by scientists and researchers who want to keep the data private and untraceable.



So not all un-indexed content is "illegal" or harmful, the Deep Web is not illegal, it is purely "non-indexed" content, nothing more.

There is a parallel Internet you may not have run across yet only accessed by a special Dark Web browser and home to a freewheeling collection of sites for everything from anonymous activism to illicit activities. Not to mention regular people who do not wish to be surveilled, or keep their identities secret.

The Dark Web (sometime called the DarkNet) is a small portion of the Deep Web that has been intentionally hidden and is inaccessible through standard web browsers. Dark Webs or hidden site, include Freenet[3] and Tor, or The Onion Router.

https://www.torproject.org/

The Tor network is an anonymous network that can only be accessed with a special web browser, called the Tor browser. The websites limited to the Tor network have a special .onion address extension like darkweba6le5w52w.onion.

Because of this, Tor's Dark Web is also known as onionland. It is an encrypted network built on top of the existing Internet. This is the portion of the Internet most widely known for illicit activities because of the anonymity associated with the Tor network. Although the Dark Web has some nebulous uses, most uses are innocuous. For example, people who want to communicate and associate online without fear of being shut

[3] *Freenet is a peer-to-peer platform for censorship-resistant communication. It uses a decentralized distributed data store to keep and deliver information, and has a suite of free software for publishing and communicating on the Web without fear of censorship. It uses your storage and bandwidth.*

down by a government agency. The Dark Web is much smaller than the Deep Web, and it is made up of numerous types of sites like Bitcoin markets, The Hidden Wiki, and porn sites. It is perhaps most notorious for its anonymous marketplaces that often sell illegal products like drugs, fake documents, and weapons.

A Dark Web is any overlay network that can be accessed only with specific software, configurations, or authorization, often using non-standard communications protocols and ports. Two typical Dark Web types are friend-to-friend networks (usually used for file sharing with a peer-to-peer connection) and privacy networks such as Tor.

The URL's or addresses, of these web sites hosted on the Tor network, are a random string of sixteen meaningless letters and numbers ranging from A to Z and 1 to 7 followed by a dot onion suffix for Version 2. Version 3 addresses are now 56 characters.

Tor or The Onion Router as you will read more of later, was developed by US Naval intelligence for military purposes, and then later became open source software.[4]

These thousands of sites are enormously difficult to shut down because of the anonymity. It is the home of whistleblowers, political activists, as well as criminal activity of illegal drugs, pornography, pirated books, media, weapons, commercial hacking services, computer exploitation software, etc.

It is also the home of creative people, because they have to be creative to be able to survive there, and so innovation takes place there as well.

It is also home to security researchers looking for information that can be obtained from monitoring Dark Web communications that suggest malicious network intrusions.

These sites can have the high quality appearance and graphics of an Amazon, eBay, or other shopping site, but rather than using a credit card, you pay via a cryptocurrency like Bitcoin.[5] The entire site is encrypted so that domestic and foreign intelligence mostly cannot see what you are looking at or what you buy.

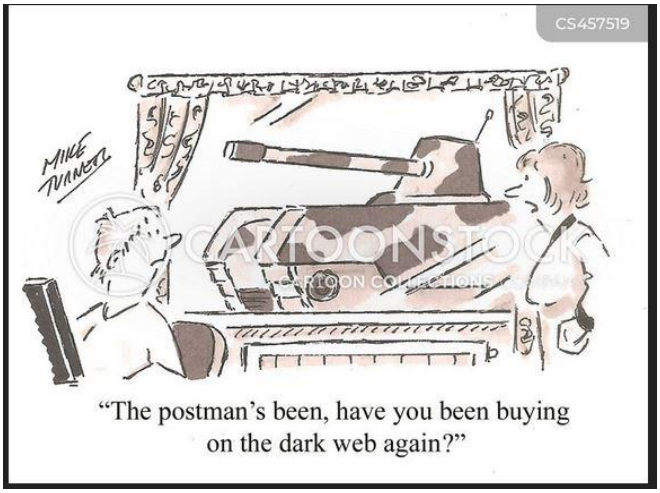
---

[4] Open-source software (OSS) is a type of computer software where source code is released under a license and the copyright holder grants users the rights to study, change, and distribute the software to anyone and for any purpose.

[5] Bitcoin is a cryptocurrency, a form of digital cash.

The sellers in these markets of course use pseudonyms, but just like the Clear Web, they too are governed by user reviews and value positive feedback from their customers. There is competition and choice in this world as well, with prices that routinely fall and quality that improves over time, with timely free shipping and generous return policies.

The Tor software provides anonymity by encrypting your IP address and routing the traffic through computers around the world designed to do this.



Many believe that it is now necessary, to surf the Clear Web with a virtual machine to protect yourself from the criminals and a Tor browser and a VPN[6] on the Dark Web to protect yourself from criminals and the NSA. A VPN alone will only encrypt the message between the two end points of the VPN tunnel allowing your ISP or any other middleman to see where you have been.

Edward Snowden speaks about surveillance and Internet freedom. The right to data privacy, is not a partisan issue, but requires a fundamental rethink of the role of the Internet in our lives — and the laws that protect it. "Your rights matter," he says, "because you never know when you're going to need them."

"Know that every border you cross, every purchase you make, every call you dial, every cell phone tower you pass, friend you keep, article you write, website you visit, email subject line you type, and data packet your router sends, is in the hands of a system whose reach is unlimited but whose safeguards are not. " NSA whistleblower Edward Snowden's encrypted email to filmmaker Laura Poitras.

https://www.youtube.com/watch?v=0dGqR4ue8dg

As Roy Zimmerman sings in his song Hello NSA, "we are fighting freedom here at home so we don't have to fight it, over there."

If you are looking for a brief version of what the Deep and Dark Webs are all about, you can read Vladimir Unterfingher's blog post and small Dark Web guide at:

https://heimdalsecurity.com/blog/how-to-get-on-the-dark-web/

[6] A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network.

OnionShare is the solution providing the anonymity cover to the users while sharing files over the Internet in a Peer-to-Peer or P2P fashion. You might have guessed by looking at the name OnionShare; it is linked to the onion network, i.e. TOR. It uses the TOR network and allows the user to share files anonymously.

Note: OnionShare: Safe Communications Stand Used By Journalists And Whistleblowers Covers Data Exposure Bug

https://darkweblink.com/onionshare/

Warning: Leaving your identity in the Dark Web makes it easy to trace you in the ClearWeb, monitor your actions, and by logging your IP they can show targeted advertising (based on your searches) or send malware. It is best to adopt a separate identity in the Dark Web.

ClearScore Protect, a London based Dark Web monitoring service only available in the United Kingdom, South Africa, and Australia.

https://www.clearscore.com/learn/protect/dark-web-monitoring-with-clearscore-protect-for-you-for-free-forever

As famed NSA whistleblower Edward Snowden once put it: *"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."*

God
@TheTweetOfGod
Mark Zuckerberg is one of the last people you should trust, and I mean that both literally and alphabetically.
1:42 PM · Mar 21, 2018
12,905 Retweets
50,321 Likes

What is considered personal data under the EU GDPR?

The European Union's General Data Protection Regulation (GDPR) tries to strike a balance between being strong enough to give individuals clear and tangible protection while being flexible enough to allow for the legitimate interests of businesses and the public. As part of this balancing act, the GDPR goes to great lengths to define what is and is not personal data.

https://gdpr.eu/eu-gdpr-personal-data/

Navigating the Dark Web

Or the

DARK SIDE OF CYBERSPACE

When was the Dark Web invented?

The term "Dark Web" was officially coined on 20 March 2000. It came with the introduction of the Freenet decentralized network system invented by Ian Clarke[7]. The intention aimed at offering access to a network that was more difficult for official sources to spy or intrude on.

To be anonymous on the Dark Web you need an anonymizer like Tor the onion router, which is a web browser, and the only way you can view the onion sites. But even then, your ISP, Internet Service Provider may see your location address and will sometimes block (i.e. Comcast) users of TOR, as they fear that you might be engaged in illegal behavior. So you will need to be anonymous to them as well by using a VPN or Virtual Private Network and connecting to it first before starting Tor.

Think of it this way, if you send a message or request a website address across the Internet, anyone who processes it can see your location, content, and destination of clear text. If you encrypt your content and spoof your location (TOR), only your ISP can see your source and destination address. However, since the Final leg from the Tor exit node is clear text, a VPN will encrypt all the way to the destination site.

If you use a VPN, your ISP cannot see your traffic, just that you are using a VPN. Your VPN provider can see you however.

[7] *Ian Clarke is the original designer and lead developer of Freenet.*

How deep is the Deep Web?

According to data from Wikipedia in the year 2000, superficial Internet had a size of 167 Terabytes, while the Deep Web had a size of 7,500 Terabytes, which means that the content of the Deep Web (which contains the Dark Web) was 45 times greater than the information to which we have direct access. Currently, the University of California at Berkeley estimates that the actual size of the deep network is 91,000 Terabytes.

Note: you should use a VPN that does not create log files, which could be legally subpoenaed. A free VPN might be collecting data from you, so chose your provider carefully.

Note: The NSA can store encrypted data in their datacenter in Utah, waiting for later, many years perhaps, for processing with more powerful quantum computers to beat the encryption.

Things you should know:

- Who owns the Tor exit nodes and are they logging all the traffic through it?
- If your computer is infected, or the cyber café being used (not recommended) is, you are screwed.
- If any servers you connect to are compromised, you are screwed.

https://answersgood.com/who-made-the-dark-web

Are there bad things on the Dark Web?

According to Peter Yeung, a writer for Motherboard magazine, the Dark Web offers idealism, lightheartedness, and community as well as the illegal, immoral, and grotesque.

Besides selling personal data and compromised accounts, cybercriminals also trade and sell the elements for needed to launch cyber-attacks, espionage, and other malicious activities on the Dark Web:

- **Off-the-shelf software exploits (exploit kits)** – toolkits that cybercriminals use to attack vulnerabilities in systems so they can then distribute malware.
- **Ready-to-use malicious software (malware)** – ransomware, information stealers, Keyloggers (to record every key pressed on a device), spyware, adware, rootkits (notoriously difficult to spot and stop), Trojans, and worms (with self-replicating capabilities).
- **Malware-as-a-service** – a subscription-based model that rents the software and hardware cybercriminals need to carry out attacks, complete with malicious software, a distribution network, a range of targets and even technical support, and a personal dashboard to manage the project.
- **Software vulnerabilities -** unknown to the software maker (called zero-days). Cybercriminals can use this to infiltrate organizations without being easily spotted.
- **Access to networks of compromised devices (botnets)** - which supply the computing resources malicious hackers need to carry out their attacks.
- **Distributed denial of service (DDoS)** - offerings which pool the power of extensive botnets to flood victims' systems with so much traffic that it takes them offline along with the services they supply.
- **Cybercriminal training -** via tutorials, guides, and other types of content that support the upskilling of bad actors.
- **Money laundering (money mulling) -** enables scammers to move around the money that they steal, extort, or otherwise take

from their victims — and turn it into clean, untraceable cash.

https://www.aura.com/learn/dark-web

Keystroke Logging and Keyloggers

Keyloggers are built for the act of keystroke logging — creating records of everything you type on a computer or mobile keyboard. These are used to quietly monitor your computer activity while you use your devices as normal. Keyloggers are used for legitimate purposes like feedback for software development but can be misused by criminals to steal your data.

https://www.kaspersky.com/resource-center/definitions/keylogger

https://en.wikipedia.org/wiki/Keystroke_logging

Anti-keylogger Software

An anti-keylogger (or anti–keystroke logger) is a type of software specifically designed for the detection of keystroke logger software; often, such software will also incorporate the ability to delete or at least immobilize hidden keystroke logger software on a computer. In comparison to most anti-virus or anti-spyware software, the primary difference is that an anti-keylogger does not make a distinction between a legitimate keystroke-logging program and an illegitimate keystroke-logging program (such as malware); all keystroke-logging programs are flagged and optionally removed, whether they appear to be legitimate keystroke-logging software or not. The anti-keylogger is efficient in managing malicious users. It can detect the keyloggers and terminate them from the system.

https://en.wikipedia.org/wiki/Anti-keylogger

One such software available is the free version of SpyShelter. It runs in the background as a tray icon in Windows.

https://www.spyshelter.com/

Botnets

Botnets are networks of hijacked computer devices used to carry out various scams and cyberattacks. The term “botnet” is formed from the word’s “robot” and “network.” Assembly of a botnet is usually the infiltration stage of a multi-layer scheme. The bots serve as a tool to automate mass attacks, such as data theft, server crashing, and malware distribution.

https://www.kaspersky.com/resource-center/threats/botnet-attacks

https://en.wikipedia.org/wiki/Botnet

Onion Links

Onion Links are the Domain name extensions in the Dark Web. Just like .com, .us, .org, .in, .net etc. that all are familiar with, .onion is the TLD of Dark Web. You cannot access .onion domains via the Clear Web because this TLD (Top Level Domain) exists only in Dark Web. You will need to use a Tor browser and the Tor network to browse .onion sites.

The good thing about .onion websites is that even if it implements cookies to track you, it cannot. Why? Simply because the onion site itself is hosted on, Tor relays. The traffic from Tor relays to onion are coming from different locations and joins together at the destination.

Each onion site has a public key and private key (similar to APIs in Clear Web) Tor network connects users to websites by following its public key.

Some mandatory rules for staying totally anonymous in the Dark Web.

The 1st Rule: **Never skip any of the rules mentioned below. Skipping any one rule can lead to revealing your true identity.**

2: Never sign up on any onion website with your Clear Web email id or username. i.e.: Do not use Gmail, Yahoo, Outlook, or any email provider on the Dark Web. Create a Dark Web email id using the services, which we will discuss later in this article. Make sure that email address does not contain your name or anything that relates to you.

3: Keep your mind clean. Dark Web is a lure. It potentially offers services of hackers, hitmen, chemical assassins, illegal drug sales, and uncensored trolls. You can explore every part as you wish. But never get deeply involved – There is no one to save you in Dark Web.

4: Disable JavaScript & cookies in your browser.

5: Use a secure operating system-**Never use Windows** 8, 10, or 11. Windows 10 particular is dangerous because of Cortana. Information about the software you use and time of using it are sent. Keyboard inputs, mouse clicks are logged and continuously transmitted back to MS servers as what they call telemetry.

When you use Linux, make sure that you avoid Ubuntu and try some lesser-known Linux distros. Or use Tor's own Linux distribution-Tails.

The chapter on Operating Systems will provide more details.

A Short History of Tor

Tor is based on the principle of "onion routing" which was developed by a team led by Paul Syverson, and included Michael G. Reed and David Goldschlag at the United States Naval Research Laboratory in the 1990's. This was based on the work of inventor and cryptographer Dr. David Chaum in the early 1980s who foresaw and upcoming privacy problem with the Internet. He wanted to eliminate the possibility of future mass surveillance and focused specifically on email. He used encryption to not only protect the contents of the message but also the metadata about source and destination using what is called a Chaum Mix.[8]

The alpha version of Tor, named 'The Onion Routing Project' or simply TOR Project, was developed by Roger Dingledine and Nick Mathewson. It was launched on September 20, 2002. Further development was carried under the financial roof of the Electronic Frontier Foundation (EFF).

The Tor Project Inc. is a non-profit organization that currently maintains Tor and is responsible for its development. The United States Government mainly funds it, and further aid is provided by Swedish Government and different NGOs & individual sponsors.

---

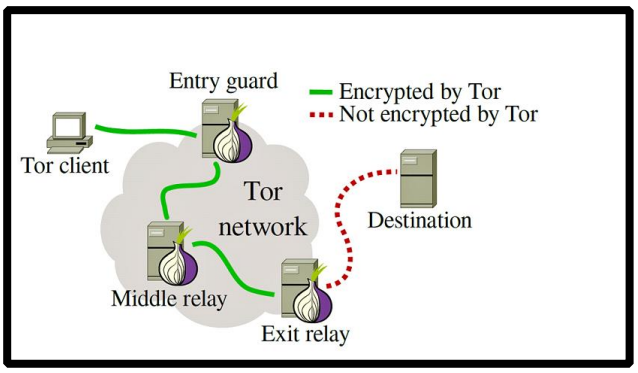
[8] *David Lee Chaum (born 1955) is an American computer scientist and cryptographer. He is known as a pioneer in cryptography and privacy-preserving technologies, and widely recognized as the inventor of digital cash.*

https://en.wikipedia.org/wiki/David_Chaum

ART: MOLLY CRABAPPLE
WORDS: JOHN LEAVITT
WHAT IS TOR?
The Internet has made it easier than ever to share information with people all over the world. But it also makes it easier for governments to track and monitor their citizens.
OCTOPUS NOT SO GREAT!
Many governments also block their citizens from seeing certain websites. The Great Firewall of China censors websites including the New York Times, Amnesty International and YouTube.
Activists, dissidents and whistle blowers can be tracked down and silenced.
By monitoring internet use, governments can link you to your private information...
How can we circumvent government surveillance and censorship?
TOR!
Tor is divided into two parts: software that allows you to use the internet anonymously, and an open network of computers that makes it possible for that software to work.
When you use Tor, your IP address remains hidden. It appears that your connection is coming from the IP address of a Tor exit relay, which can be anywhere in the world.
The Tor Software depends on the Tor network, which is made up of Tor relays run by individuals all over the world. The more Tor relays we have running, the faster the network runs and the more secure and robust it becomes.
But what can you do? Join EFF's Tor challenge. Run a Tor relay to encourage the spread of freedom and protect the anonymity of Tor users all over the world.

Tor Project's mission statement: "To advance human rights and freedoms by creating and deploying free and open anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding."

Tor works on the concept of 'onion routing' method in which the user data is first encrypted and then transferred through different relays present in the Tor network, creating a multi-layered encryption (layers like an onion), keeping the identity of the user safe.



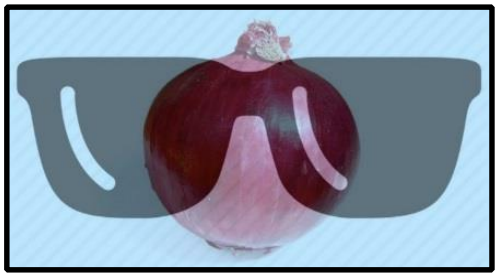
One encryption layer is decrypted at each successive Tor relay (server), and the remaining data is forwarded to any random relay until it reaches its destination server. For the destination server, the last Tor node/exit relay appears as the origin of the data. It is hard to trace the identity of the user or the server by any surveillance system acting in the mid-way, since your route changes every approximately ten minutes.

Other than providing anonymity to standalone users, Tor can also provide anonymity to websites and servers in the form of Tor Hidden Services. Tor is the network of routers or relay nodes that helps users to stay anonymous by routing the Internet traffic through different nodes. The destination website cannot access the exact location of you because your IP address

has been masked by the Tor nodes. Each time, the user visits the site; the apparent location of his/her is changed. Tor relay nodes are provided only the IP of the next node and the previous node from which it obtained the traffic.

Location is an important aspect in the Internet, which helps to track you. Normal website cookies can track accurately to your city. But specialized malware bots can access your exact address based on your searches, and your browser cache. Tor enabled browsers do not store cookie data nor allow JavaScript to run.

Essentially, Tor acts as the godfather of Dark Web websites. Each Dark Web server is connected to Tor relays directly so that the Clear Web (Clear Web is the normal Internet that we use) search engines fail to index their Universal Resource Locators or URLs.



Note: There are rumors that the government is working on, or currently using, a Google for the Dark Web called Memex (memory index), to be able to find criminal activity.

TOR encrypts your connection, not your data. So, if you are sending some 'plaintext' information, then at the exit node, where the last layer of encryption is decrypted, the vulnerability exists that someone might access your unprotected data. So, it is advised that you can also use HTTPS (encrypted) connections to safeguard your data while it is on its way to the destination server. (See a discussion of this that follows)

Try not to send any confidential information like your email, phone, or other personal details without any encryption, as it might serve as the means to identify you, no matter how many relays you have jumped through.

Traffic Fingerprinting is a method used to analyze web traffic by analyzing the patterns, responses, and packets in a particular direction. This technique can be used to attack the

Tor network by making the attacker's computer act as the guard. The main vulnerability was found at its exit points where the level of security is compared to the rest of the Tor network.

Traffic fingerprinting is a technique used to sniff the web traffic by analyzing the data packets' flow pattern- without removing the encryption. This technique has been recently used successfully to break the layers of anonymity of the Tor network users and hidden services. More information on this subject follows.

Tor Bridges

Like ordinary Tor relays, bridges are run by volunteers; unlike ordinary relays, however, they are not listed publicly, so an adversary cannot identify them easily. Using bridges in combination with pluggable transports helps to conceal the fact that you are using Tor, but may slow down the connection compared to using ordinary Tor relays.

https://tb-manual.torproject.org/bridges/

What is a bridge?

Bridge relays are Tor relays that are not listed in the public Tor directory.

That means that ISPs or governments trying to block access to the Tor network cannot simply block all bridges. Bridges are useful for Tor users under oppressive regimes, and for people who want an extra layer of security because they are worried somebody will recognize that they are contacting a public Tor relay IP address.

A bridge is just a normal relay with a slightly different configuration. See how do I run a bridge for instructions.

Several countries, including China and Iran, have found ways to detect and block connections to Tor bridges. Obfsproxy bridges address this by adding another layer of obfuscation. Setting up an obfsproxy bridge requires an additional software package and additional configurations. See our page on pluggable transports for more info.

https://support.torproject.org/censorship/censorship-7/

Tor Browser Now Bypasses Internet Censorship Automatically (bleepingcomputer.com) 15

Posted by BeauHD on Friday July 15, 2022 @06:40PM from the new-and-improved-features dept.

An anonymous reader quotes a report from BleepingComputer: The Tor Project team has announced the release of Tor Browser 11.5, a major release that brings new features to help users fight censorship easier. [...] The updates in Tor Browser 11.5 focus on circumventing censorship, a process that started a year ago in version 10.5 with improving the Tor connection experience. In the new version, users no longer have to manually try out bridge configurations to unblock Tor.

Tor Browser version 11.5 comes with a new feature called "Connection Assist," which assigns automatically the bridge configuration known to work best for the user's location. "Connection Assist works by looking up and downloading an up-to-date list of country-specific options to try using your location (with your consent)," explains the release announcement. "It manages to do so without needing to connect to the Tor Network first by utilizing moat – the same domain-fronting tool that Tor Browser uses to request a bridge from torproject.org." Since Connection Assist is still in an early stage of development (v1.0), the Tor team welcomes user feedback and reports, which would help them iron out any kinks and improve on the system.

Another important new feature in version 11.5 is making 'HTTPS-Only Mode' the default browsing mode, so that the connection is through a secure tunnel. This ensures that all data exchange between the user and the server hosting the website will be encrypted, to defend against man-in-the-middle (MitM) attacks and to protect users from SSL stripping on malicious exit relays. [...] The third significant improvement in Tor Browser 11.5 is a heavily revamped Network Settings menu, now called "Connection Settings," which should make it easier to find and understand specific settings. Most notably, bridge configuration and connection options have been redesigned to enable quick and easy review and management. Using emojis on the saved Bridges, the new interface offers visualization for the configuration for the first time, making it easy to identify the right bridge and select it when needed. You can download the latest Tor Browser from the official download portal.

How Tor Is Fighting—and Beating—Russian Censorship

Russia has been trying to block the anonymous browser since December—with mixed results.

https://www.wired.com/story/tor-browser-russia-blocks/

TorStatus - Connection stats.

http://t3qi4hdmvqo752lhyglhyb5ysoutggsdocmkxhuojfn-62ntpcyydwmqd.onion/

Map of all Tor Relays

Map of all Tor Relays at tormap.void.gr

(The orange dots are the bad nodes, avoid them by any and all means)

As of 2021 there are more than 7500 Tor relays being run. 2800 of those are hosted in Germany and the USA. There are an estimated eight million daily worldwide users.

Let us hear with the DW'ers have to say about Tor on the DarkWeb dread forum.

Bad Tor Relays

Posted by /u/darknetinside • in dread forum /d/Council

As many asked what that is and how to spot a bad relay, I paste here the definition and a few links to tools from the torproject.org

Ran into a misconfigured, malicious, or suspicious relay while using Tor? Please let us know by sending email to bad-relays AT lists DOT torproject DOT org! Many bad relays are caught thanks to our wider community, so many thanks for all your help and vigilance!

What is a bad relay?

A bad relay is one that either doesn't work properly or tampers with our users' connections. This can be either through maliciousness or misconfiguration. Some common examples are...

Tampering with exit traffic in any way (including dropping accepted connections). This might be accidental (such as an anti-virus filter) or malicious (commonly SSLStrip, which replaces https:// links with http:// to snoop on traffic) or even intentional (such as layer 7 inspection for P2P traffic detection/mitigation).

Running HSDirs that harvest and probe .onion addresses

Manipulating the DHT that is used for onion services, e.g., by positioning itself in the DHT.

Using a DNS provider that censors its results (such as some OpenDNS or Quad (9.9.9.9) configurations).

Performing a Sybil attack, which means flooding the network with new relays in an effort to deanonymize users. If you want to run multiple relays then that's great! But please be sure to set the MyFamily parameter.

Exit relays routing their exit traffic back into the tor network (not actually exiting any traffic)

Also, if your relay is stolen or goes missing, please report it as well, so we can blacklist it in case whoever took it puts it back online.

The following are currently permitted yet do have some discussion for prohibition (as such, they should not be reported at this time)...

Only allowing plain-text traffic (for instance, just port 80). There's no good reason to disallow its encrypted counterpart (like port 443), making these relays highly suspect for sniffing traffic. See context and spec.

How do I report a bad relay?

]If you encounter a bad relay then please let us know and write to bad-relays AT lists DOT torproject DOT org.

You can check which exit you are using at any time by visiting tor check. Please include the following in your report:

The relay's IP address or fingerprint. The fingerprint is a forty-character hex string such as 203933ED4E55EF8A3C3518427D1A1ED6A4CC285E.

What kind of behavior did you see?

Any additional information we'll need to reproduce the issue.

However, if you need help with anything Tor-related, please contact the front desk instead.

What happens to bad relays?

After a relay is reported and we've verified the behavior we'll attempt to contact the relay operator. Often we can sort things out but if not (or the relay lacks contact information) we'll flag it to prevent it from continuing to be used.

We have three types of flags we can apply:

BadExit - Never used as an exit relay (for relays that appear to mess with exit traffic)

Invalid - Never used unless AllowInvalidNodes is set (by default this only allows for middle and rendezvous usage)

Reject - Dropped from the consensus entirely

Which we use depends on the severity of the issue, and if it can still be safely used in certain situations.

My relay was given the BadExit flag. What's up?

In just about all cases we're unable to contact the operator to resolve the issue, so if your relay has been flagged as a BadExit then please let us know (see above for contact info) so we can work together to fix the issue.

Map of all Tor Relays at tormap(dot)void(dot)gr (the orange dots are the bad nodes, avoid them by any meaning)

Tortunnel github(dot)com/moxie0/tortunnel

tortunnel is a partial Onion Proxy implementation that's designed to build single-hop circuits through Tor exit nodes. This is useful in cases where you might want some very low level of anonymity and don't want to deal with the performance implications of using Tor's full three-hop circuits.

tortunnel exposes itself both as a SOCKS interface, as well as a fairly clean asynchronous C++ API to the Tor protocol itself. It was first written as a scanning tool for checking to see whether exit nodes were running sslstrip, and is well suited for implementing other high-performance scanning routines against the Tor network as a whole.

It might also be useful for implementing a perspectives-like interface for checking SSL, SSH, or other host certificates. It could be useful as an nmap scanning mode, or perhaps for something else entirely.

To expose a SOCKS interface on localhost:5060 to a random one-hop Tor exit node, run:

torproxy -p 5060 -r

To expose a SOCKS interface on localhost:5060 to a specific Tor exit node IP address, run:

torproxy -p 5060 -n

These commands will open a SOCKS interface on localhost:5060, which you can then point applications which support SOCKS proxies to. Be careful, though, remember that this is not useful for anything approaching strict anonymity requirements.

To see if it works, you can try a "curl --socks5 localhost:5060 ifconfig(dot)me" and compare it with the output of "curl ifconfig(dot)me".

Finally the tool to pick your own preferred Tort entry middle and exit nodes is named Selektor and is implemented in many Linux distributions (handle with care and if you don't know what you do, don't use it, you might make it worse)

This is what a Tor upgrade alert looks like, and following dread message thread.

[PSA] Serious security vulnerability in TOR BROWSER [ALL VERSIONS AFFECTED]

by /u/HugBunter A in /d/OpSec

Upgrade Tor Browser to the latest release (11.0.13) immediately where possible and ensure you have JavaScript Disabled in Tor Browser at all times, as always. This vulnerability is present in Firefox, and so affects all previous Tor Browser versions < 11.0.13. Affects all platforms, including Tails, as detailed in their warning below. They cannot currently push an emergency release for Tails specifically, will be resolved with a Tor Browser update in Tails 5.1 on May 31.

https://tails.boum.org/security/prototype_pollution/index.en.html

Tor Browser in Tails 5.0 and earlier is unsafe to use for sensitive information.

We recommend that you stop using Tails until the release of 5.1 (May 31) if you use Tor Browser for sensitive information (passwords, private messages, personal information, etc.).

A security vulnerability was discovered in the JavaScript engine of Firefox and Tor Browser. See the Mozilla Foundation Security Advisory 2022-19

This vulnerability allows a malicious website to bypass some of the security built in Tor Browser and access information from other websites.

For example, after you visit a malicious website, an attacker controlling this website might access the password or other sensitive information that you send to other websites afterwards during the same Tails session.

This vulnerability doesn't break the anonymity and encryption of Tor connections.

For example, it is still safe and anonymous to access websites from Tails if you don't share sensitive information with them.

After Tor Browser has been compromised, the only reliable solution is to restart Tails.

Other applications in Tails are not vulnerable. Thunderbird in Tails is not vulnerable because JavaScript is disabled.

The Safest security level of Tor Browser is not affected because JavaScript is disabled at this security level.

Mozilla is aware of websites exploiting this vulnerability already.

This vulnerability will be fixed in Tails 5.1 (May 31), but our team doesn't have the capacity to publish an emergency release earlier.

http://pzhdfe7jraknpj2qgu5cz2u3i4deuyfwmonvzu5i3nyw4t4bmg7o5pad.onion/new-release-tor-browser-11013/index.html

Tor Browser 11.0.13 is now available from the Tor Browser download page and also from our distribution directory.

This version includes important security updates to Firefox.

We also updated Tor to 0.4.7.7 (the first stable Tor release with support for congestion control).

Note: the Android version 11.0.13 will be available later during the week.

The full changelog since Tor Browser 11.0.12 is:

Android

Bug fenix#40212: Tor Browser crashing on launch

All Platforms

Update Tor to 0.4.7.7

Bug tor-browser#40967: Integrate Mozilla fix for Bug 1770137

Bug tor-browser#40968: Integrate Mozilla fix for Bug 1770048

Build System

All Platforms

Update Go to 1.17.10

Bug tor-browser-build#40319: Add build tag to downloads.json

Bug tor-browser-build#40486: Add tools/signing/do-all-signing script, and other signing scripts improvements

/u/HeadJanitor Moderator

https://blog.torproject.org/new-release-tor-browser-11013/

Tor Browser 11.0.13 is now available from the Tor Browser download page and also from our distribution directory.

This version includes important security updates to Firefox.

We also updated Tor to 0.4.7.7 (the first stable Tor release with support for congestion control).

Note: the Android version 11.0.13 will be available later during the week.

The full changelog since Tor Browser 11.0.12 is:

Android

Bug fenix#40212: Tor Browser crashing on launch

All Platforms

Update Tor to 0.4.7.7

Bug tor-browser#40967: Integrate Mozilla fix for Bug 1770137

Bug tor-browser#40968: Integrate Mozilla fix for Bug 1770048

Build System

All Platforms

Update Go to 1.17.10

Bug tor-browser-build#40319: Add build tag to downloads.json

Bug tor-browser-build#40486: Add tools/signing/do-all-signing script, and other signing scripts improvements

/u/HeadJanitor Moderator

What we are waiting on:

CVE-2022-1802: Prototype pollution in Top-Level Await implementation

If an attacker was able to corrupt the methods of an Array object in JavaScript via prototype pollution, they could have achieved execution of attacker-controlled JavaScript code in a privileged context.

CVE-2022-1529: Untrusted input used in JavaScript object indexing, leading to prototype pollution

An attacker could have sent a message to the parent process where the contents were used to double-index into a JavaScript object, leading to prototype pollution and ultimately attacker-controlled JavaScript executing in the privileged parent process.

/u/TTTz P Master of Arts

TorProject Onion link -

http://pzhdfe7jraknpj2qgu5cz2u3i4deuyfwmonvzu5i3nyw4t4bmg7o5pad.onion/new-release-tor-browser-11013/index.html

/u/HugBunter A

Thanks, added that link instead.

/u/foshizzledizzle

well at least we got 'congestion control' now.

/u/newbieforever2018 "You've got ★bail★"

And you make fun of me using Windows OS?

/u/HeadJanitor Moderator

Debian just brainwashes you into checking for updates every hour, just to see it happen.

/u/decaptchamyass

Don't tell me that you are using debian as a daily driver.

/u/HeadJanitor Moderator

I use a Type 1 hypervisor so I'm switching from one OS to another throughout the day. Debian Stable brings the calm.

/u/TTTz P Master of Arts

There was just a 2v update to TB from 11 - 13

/u/HugBunter A

Didn't see it, will amend the post

/u/decaptchamyass

Exactly. Also why he is linking Tails blog post? If there is a critical vuln, I wouldn't trust anyone but torproject to notify everyone.

/u/HugBunter A

Because Tor Browser upgrades within Tails for your average user, require a Tails upgrade, which isn't going to be available until May 31. A good portion of users will be using Tails, so this applys to them mainly to ensure they have JS disabled and upgrade as soon as possible. Other platforms will be notified of an upgrade for Tor Browser.

Tor also did not release a blog post detailing the vulnerability and simply linked the FIrefox bug tracker for the issue. This explains the severity and I was notified of it by someone sending me this link.

And so you edited your comment to save face after my explanation...

/u/decaptchamyass

You edited the post, don't tell me that. It doesn't make sense to first link an article from an inherently insecure OS and then add the official source.

/u/HugBunter A

Re-edited 4 minutes ago, the timestamps are visible to everyone..

/u/HugBunter A

Edited the post to update with the Tor upgrade change log yes, because I didn't see the upgrade while quickly putting this PSA up, completely unrelated to what you said.

/u/HugBunter A

Can you stop editing your comments and instead add a separate reply? It does when the main issue here is how differently this affects Tails users, as to other's who's OS' don't necessarily inhibit the upgrade process to Tor Browser.

/u/decaptchamyass

Your title was misleading, that's all I am saying.

/u/HugBunter A

I agree it was, the post was made in haste. However, all previous Tor Browser versions are susceptible and I believe this vuln has been leveraged within our community previously, at least 3 months ago. It lines up with some vendor and buyer information that was shared by a phisher, claiming to be using a JS exploit.

/u/Cannabel P

I had a thought, that the Coincollector guy had taken over Williamgibsons account. This is of course only speculation on my side but writing style and the fact he sent the phishing links on market with WilliamGibsons name to all vendors claiming they were private mirrors + williamgibson only replied to his thread here on dread and the coincollector recommended gibson to keep all the xmr of versus users and split it between the team. Just connecting dots.

/u/adruguser

haha the phishing email coincollecter sent was so obvious. the signature didnt check out, and the account had a space in the name

/u/Cannabel P

Okay then he might did not use this JS vulnerability.

I also saw that the signature didnt match when i checked the message. Didnt see the space in his name at that time though.

/u/decaptchamyass

Well, this isn't going to change unless Tor Browser migrates to Chromium. Tails cannot upgrade Tor Browser without an update itself describes how unreliable it is, not mentioning the countless critical

vulnerabilities that have been found in the past.

/u/formenot123

Glad to see I'm not the only one that gets pissed off at people editing previous comments. I still think should have max edit character limit of like 20. So /u/fudpolice doesn't trick me by editing his previous comments again.

/u/TTTz P Master of Arts

[removed]

/u/decaptchamyass

[removed]

/u/TeddyBaby

Please shut the fuck up

/u/BillClinton

so if i disable java via config am i still safe? on tails. im a bit green, sorry.

thanks for bringing this to our attention

/u/HugBunter A

As long as you are using the safest security setting in Tor Browser, you should be unaffected as this disabled JavaScript. If you want to make sure JS is completely unavailable in the browser at the engine level, you can disable it by entering "about:config" in the address bar, and search for "javascript" on that page, you should see "javascript.enabled", you can double click this to set the value to "false".

/u/BillClinton

thanks, hug. big love

/u/flowersinbloom

TY again. Top work :)

/u/AlphaZero

And as your aptly-positioned moderator of /d/OpSec /u/headjanitor points out, 9 times out of 10, when you click 'SAFEST' - then go check about:config after switching to 'safest' - you'll notice Mozilla was nice enough to still nonetheless keep Java enabled for you!

/u/HugBunter A

The safest security mode disables JavaScript at run-time through the NoScript plugin in the Browser. The JavaScript.enabled value is the browser engine level setting for JavaScript, which cannot be altered by a plug-in as far as I know. So it is separate. There have been instances of NoScript failing due to a bug in previous releases, so disabling at the engine level would prevent any issues with NoScript failing.

All in all, the value in about:config is separate and will always remain true even when your security settings have disabled JS via NoScript.

/u/AlphaZero

Seriously man, thank you for the well-articulated reply correcting my gap in knowledge - perfect.

/u/KyleKlemons54

Just did that Hug. Thanks.

/u/elcalaveira

I'm glad this vulnerability is easily avoided by disabling JavaScript as this is the basic standard for dark web surfing.

/u/foshizzledizzle

Tails doesnt even have the competence to put this on their homepage.

/u/kwoon

This warning is the first thing I saw when I launched OS.

/u/legallybraindead

Does this have any relation in what is going on with the market's dropping like flies right now?

/u/HugBunter A

No relation and this is the usual cycle for markets

/u/hustlinwithheart

Guys I recently had a order accepted by a vendor on versus market that had 4,500 USD in bitcoin on it. The vendor says he isnt shipping me my gear because he didnt get the money. I also read that "Accepted orders will be paid out to the vendor while pending orders will be refunded to the customer." Does this mean that the vendor will be getting my money instead of the moeny being refunded back to my wallet? Any reply would be greatly appreciated im panicking about losing all this money :(

/u/Reckless

This is not at all the place for this question.

I'll just cut to the chase: Your money is gone and you're not getting it back. The vendor said he's not sending it to you, if it wasn't marked shipped there's absolutely nothing you can do. If it was in a Pending status, you MIGHT get it back, but don't count on it. Even markets that have exit gracefully haven't done so as gracefully as they have stated outwardly.

/u/We_Are_9000

So just Tails??? My browser updated this morning in Whonix, so I'm OK???? Why just Tails & not Whonix or any other OS??? Or am I just reading too much into it??? I just woke up :P

/u/brokenbox

How do I update TAILS? I'm worried I'll lose my persistent storage. I keep getting the pop-up window suggesting I update TAILS but I have no idea how frankly.

/u/KyleKlemons54

SO basically I need to wait a week before using TAILS again? Alright. Thanks Hug.

/u/Cannabel P

No, you can browse as you did in the 'safe mode'.

/u/KyleKlemons54

Well I'm using "safest mode" and I also followed Head Janitor's advice

in some of the comments above. i.e. the about:config thing. I will keep doing this until the bug is fixed. Thanks for the heads up though m8. Appreciate it.

/u/AlphaZero

PLEASE - FIND JA RULE! GET AHOLD OF THIS MOTHAFUCKA SO I CAN MAKE SENSE OF ALL THIS

/u/OfficialJabberJaw

The Safest security level of Tor Browser is not affected because JavaScript is disabled at this security level.

As long as you have java disabled (which you should) you will be fine

Dark Web.wtf

Dark Web.wtf is a safe resource for easy access to the DarkNet with TOR or other .ONION browser. I list sites I trust on the DarkNet and as soon as there is a scam alert or some sort of warning I remove and disable the site. Using my site means safe access to DarkNet without remembering or copying long random-looking .ONION addresses since we automatically forward you to a working one.

https://darkweb.wtf

The best links to Tor browser v3 2021

https://darkweb24.net/the-best-links-to-tor-browser-v3-2021/

Links are not sorted, you can find links to shops, email, blogs, forums, etc. Interesting that I could not find their onion site.

Only around three per cent of all Tor traffic is on the 'dark web' (.onion sites) -- many media announcements regarding the scale of hidden services and the potential for criminality are overstated.

https://go.kaspersky.com/rs/802-IJN-240/images/Dark%20Web%2010172017.pdf?aliId=521973948

Http:\\ or Https:\\ on onion sites?

From Reddit /r/TOR

I wanna know if normal http onion sites have end-to-end encryption like the clearnet https ones?

Yes, they do.

For more discussion about HTTPS on hidden services, see

https://www.reddit.com/r/TOR/comments/bg1rxr/do_tor_hidden_services_require_https_is_there_an/.

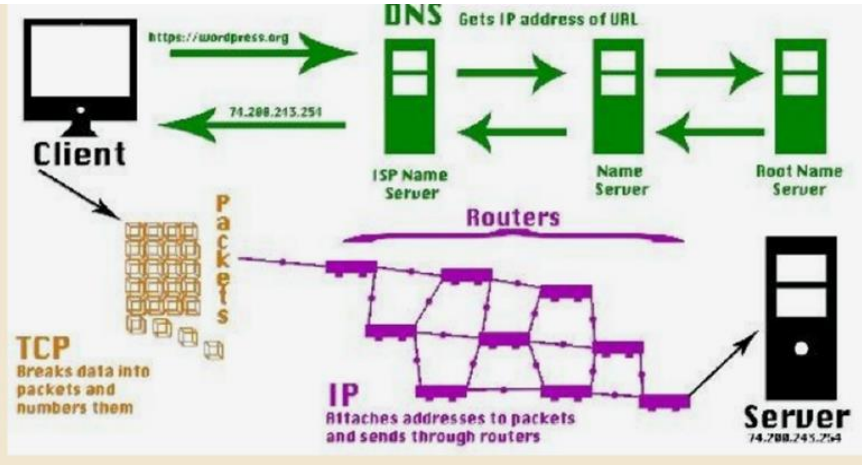
The only reason HTTPS onions exist is so there's a third-party (the certificate authority) involved in verifying the site's authenticity.

*As others have said, the **Tor protocol provides end-to-end encryption for .onion sites even with just http**. If you visit a .onion site with an unverified https certificate, that's effectively the same as visiting a http .onion site. There are some certificate authorities that have issued certificates for .onion domains, so you can get a https green lock for a .onion site (for example, https://facebookcorewwwi.onion). Arguably this has some small security benefit (Facebook I believe uses it because so their Tor instance(s?) can just forward the ssl (https) connection on to Facebook's normal webservers, which will handle the certificate), but for the vast majority of .onion sites, which run the webserver on the same server as the Tor instance, it's useless.*

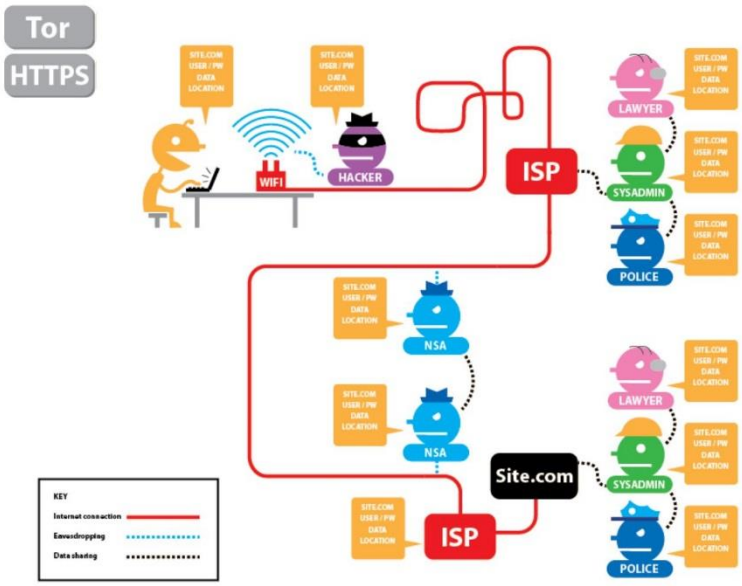
The EFF has a good write-up on this

https://www.eff.org/pages/tor-and-https

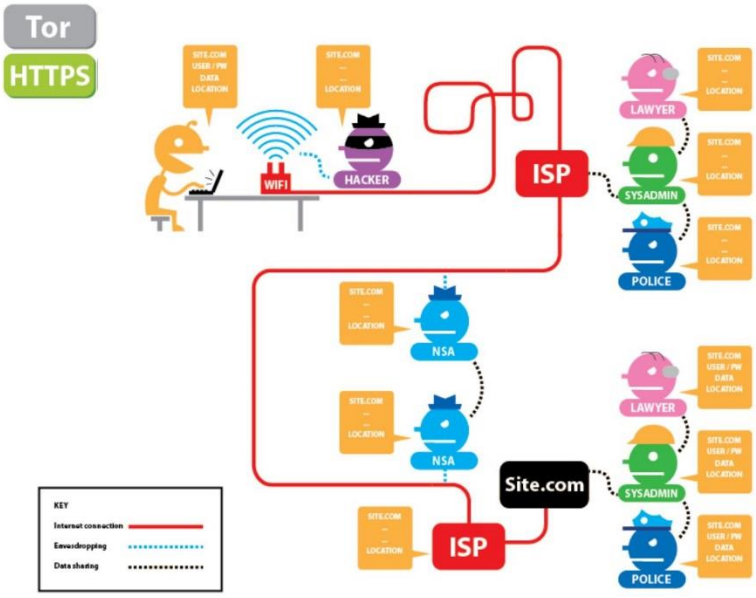
This site also has a very interesting interactive network map.



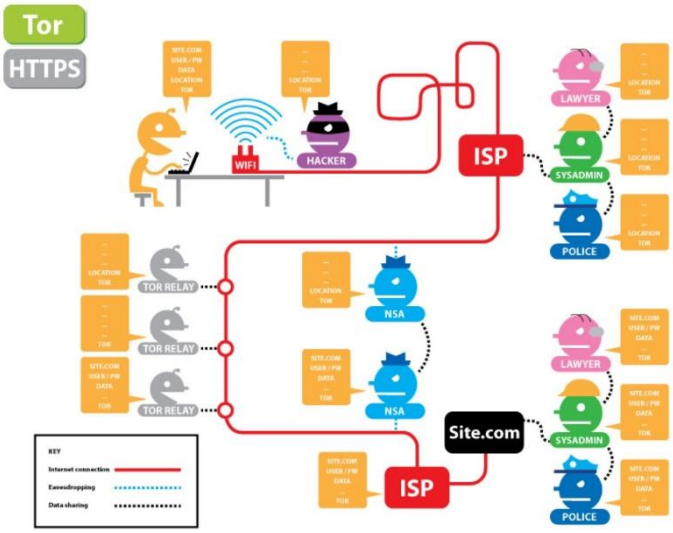
Basic Internet operation



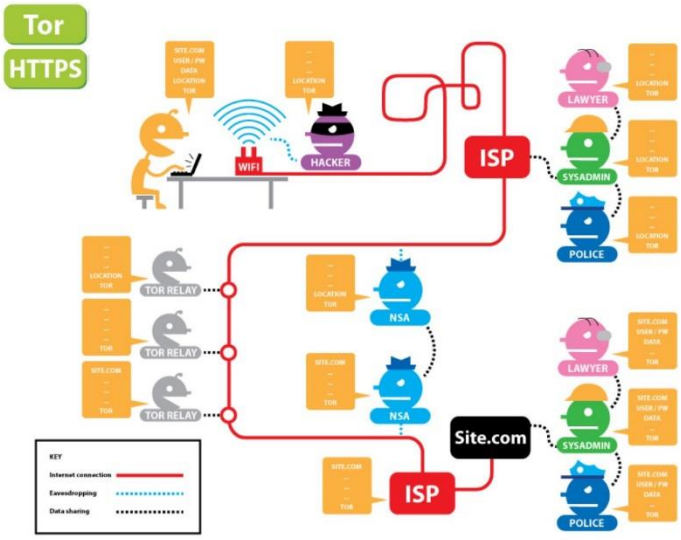
When both buttons are grey, you see the data that is visible to eavesdroppers when you do not use either tool.



Click the "HTTPS" button to see what data is visible to eavesdroppers when you are using HTTPS. The button will turn green to indicate that HTTPS is on.



Click the "Tor" button to see what data is visible to eavesdroppers when you are using Tor. The button will turn green to indicate that Tor is on.



When both buttons are green, you see the data that is visible to eavesdroppers when you are using both tools.

Note: Potentially visible data includes the site you are visiting (SITE.COM), your username and password (USER/PW), the data you are transmitting (DATA), your IP address (LOCATION), and whether or not you are using Tor (TOR).

Tor Tools

How traffic fingerprinting attacks the Tor network?

What is traffic fingerprinting? The basic website traffic fingerprinting refers to recognize the web traffic by analyzing the patterns, responses, and packets sent and received in a particular direction- everything despite the use encryption or anonymity.

How is it used to attack Tor network? The traffic fingerprinting in Tor requires that attacker's computer to act as the guard on a Tor circuit. If an attacker manages to connect many machines to the Tor network, the odds are that, on some occasion, some computer of attacker will be at the right place and at the right times to sniff the traffic.

When a Tor circuit is established, the systems on Tor network pass a huge amount of data. MIT News writes: "By looking for patterns in the number of packets passing in each direction through a guard, machine-learning algorithms could, with 99% accuracy, determine whether the circuit was an ordinary Web-browsing circuit, an introduction-point circuit, or a rendezvous-point circuit." To achieve this, breaking Tor's encryption was not necessary. Similarly, using a Tor-enabled computer, traffic analysis could identify the hidden services with 88% accuracy.

How to defend against traffic fingerprinting in Tor network.

Researchers recommend to mask the sequences to make all the sequences look identical- actually, send dummy data packets to make all different circuits look the same.

"We are considering their countermeasures as a potential improvement to the hidden service," they add. "But we think we need more concrete proof that it definitely fixes the issue."

Traffic fingerprinting in Tor network is not something that could be done over a period of few days. An attacker must spend a long time to collect data and to dig deeper into the network.

https://fossbytes.com/what-is-traffic-fingerprinting-and-how-it-is-used-to-attack-tor-network/

Learn more about Tor

https://www.torproject.org/

http://2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu-3zzui5du4xyclen53wid.onion/index.html

Tor Blog

http://pzhdfe7jraknpj2qgu5cz2u3i4deuyfwmonvzu-5i3nyw4t4bmg7o5pad.onion/index.html

What Not To Do While Using TOR

Do not use your mobile phone for 2-Step verification on Tor

Most websites provide a 2-Step verification using a mobile number in which an OTP (One Time Password) is sent to your mobile number, allowing you to safely login to your account. You need to be careful when you are using TOR browser for accessing your account.

If you provide your mobile number to a website, it will only hamper your anonymity status online as it will be easier to track you down using your number.

Note that even if you are using a SIM card registered in some other person's name, your telecom operator can easily track you down as they also keep your device's IMEI number in their database and can be used to track you.

Do not operate user accounts outside TOR

If you use TOR browser for checking your Facebook, Twitter, or email accounts, do not ever use those accounts outside the TOR browser, as it will expose your online identity to the website. Almost every site on the web now logs information like your login and logout time, your location, your IP address, and other details. Using your account on the open Internet even once will be enough to get your IP address logged and eventually reveal your identity.

Do not post your personal information

You must embed this point in your heart; do not post any personal information like name, address, birthday, credit card number while using TOR. It will uncover your identity, and there will no point using the TOR, hope you can understand.

To keep yourself completely hidden, you need to be pseudonymous. Now, what is that? It means you need to assume

yourself as a person with disparate behavior while you use TOR. The new person should have different kinds of likes and hatreds, food choices, fantasies, etc.

For that purpose, create a new user account with a new email address that does not reflect even a bit of your real identity. You can use that email for your social accounts and enjoy your anonymity and praise the power of TOR.

Also, do not confuse between anonymity and pseudonymity.

An anonymous connection is the one in which the server to which you want to connect has no idea about your real IP address/location and your identity.

A pseudonymous connection is the one in which the server which is being requested has no idea about your true IP address/location, but does have an identity it can associate with the connection.

Do not send unencrypted data over TOR

While you were reading the article about TOR, you came across the fact that TOR encrypts your connection, not your data, and TOR's exit nodes are vulnerable. So, it is highly advisable not to send unencrypted data over the TOR network, as someone might access your information while the data is on the last node.

Do not use TOR with Windows

Microsoft's Windows is the world's most used operating system for desktops, but it does not seem to do well when you would like to use TOR browser on it. The credits are bagged by the vulnerabilities that exist on the operating system and may reveal your identity even if you are using the TOR to access the Internet.

Linux systems will serve you well for this purpose. Linux distributions like Tails and Whonix are pre-configured with TOR. You can configure it manually on any distribution you may like.

Do not forget to delete cookies and local website data

When you access a website, it sends a small file to your computer, which keeps the record of your browsing habits and other data so that the website can recognize you on your next visit; the file is called a cookie. Some website may also store data locally on your hard drive.

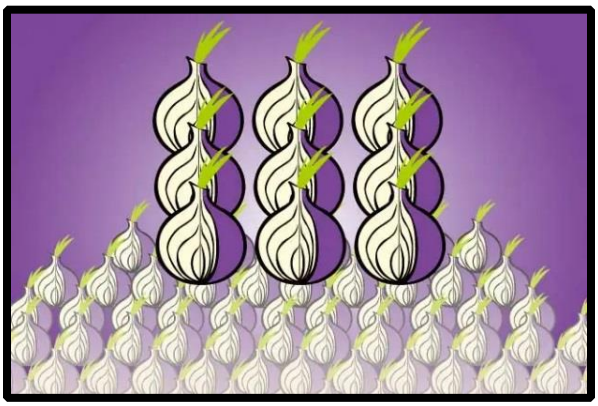
You should delete those cookie files and local website data after every browsing session you perform on TOR. These things may allow the website to gather information about you and track your location and IP address.

Later versions of Tor browser automatically deleted website cookies and download history after you end a session. Alternatively, you can click on the New Identity option (click the onion button before the address bar) to the same without closing the Tor browser.

Do not use TOR for Google Search

If you want to be anonymous while using TOR, do not use Google to search your queries. Though it sounds weird, this is because Google collects information like your search requests, stores cookie files on your computer, and tracks your browsing habits to power its advertisement services.

You do not want to reveal that, do you? So, you can use other search engines like DuckDuckGo and StartPage, as they do not log your IP address or any other activity. In fact, there have been instances where Google work properly with Tor. They might display an error message or as you to solve a captcha. That is because people reaching Google through Tor becomes seem suspicious.



Do not use HTTP website on TOR

You very well know that TOR can be exploited using the vulnerabilities that exist at its exit nodes. If you access HTTP sites using TOR, there are chances someone might access your information while it is on the end points. The data transferred to and from an HTTP site is unencrypted and can be viewed at the end points as TOR only encrypts the connection inside its network.

You can prevent such situations by the use of HTTPS websites. They use end-to-end encryption protocols like SSL (Secure Socket Layer) and TLS (Transport Layer Security). So, all your data remains safe even if it is outside the TOR network.

Do not connect to the same server with and without TOR simultaneously

Here is one important thing you need to keep in mind. If you are accessing a particular remote server using TOR (anonymously), do not access the same server from outside the TOR network (non-anonymously) as it may lead to a revelation of your actual identity. This is because in case your Internet is down, both your connections will terminate at the same moment, and it will not be much difficult for someone spying on you to relate the pieces and complete the puzzle.

Also, a web server might try to correlate the two connections by increasing or decreasing speed on one of your TOR or non-TOR connection to see whether the speed fluctuates on the other one and consequently trace your real IP address.

Tor Identities

NEW IDENTITY

This option is useful if you want to prevent your subsequent browser activity from being linkable to what you were doing before. Selecting it will close all your open tabs and windows, clear all private information such as cookies and browsing history, and use new Tor circuits for all connections. Tor Browser will warn you that all activity and downloads will be stopped, so take this into account before clicking “New Identity”.

To use this option, you just need to click on 'New Identity' in Tor Browser's toolbar.

NEW TOR CIRCUIT FOR THIS SITE

This option is useful if the exit relay you are using is unable to connect to the website you require, or is not loading it properly. Selecting it will cause the currently-active tab or window to be reloaded over a new Tor circuit. Other open tabs and windows from the same website will use the new circuit as well once they are reloaded. This option does not clear any private information or unlink your activity, nor does it affect your current connections to other websites.

You can also access this option in the new circuit display, in the site information menu, in the URL bar.

https://tb-manual.torproject.org/managing-identities/

How to verify an Onion

How to verify an Onion

by /u/Shakybeats M Modinator • 1 year ago in /d/DarknetMarketsNoobs*

Verifying onions. It's such an important thing yet so many people don't know how to do it properly. ***Always****, regardless of where you get the onion from take the time to verify it. You never know when you have a typo, or a simple error. Taking the 10 seconds to verify can save your coins from falling to a phisher.*

Darkfail has a great tool to help you do it, but no one resource should be blindly trusted. You should always ***manually*** *verify the onion address yourself!*

First lets make sure you understand how to verify a pgp signature.

Note: *If you know how to verify a signature but are unsure how to verify an onion skip down to the verifying onion part below.*

Verifying a PGP signature

Verifying a signature is very simple to do. First you need to import a PGP key from the person you want to verify. If you are unsure how to import a key visit this post

Lets verify a signature i'll make. To do this you need to import my PGP key. You can find it by clicking my profile or here

Once you have it imported highlight the text below. Including all of the dashes. You should see a red stamp on the clipboard in your upper right hand corner. Click the clipboard, decrypt/verify clipboard. You should see the message I typed on top. Then below you should see gpg: Good signature from "Shaky" along with some other information. The good signature part is all we are looking for. If you see "Bad Signature" you know something is up.

And you're done. You've verified a pgp message!

Note: *If you see the following. It just means you have not set a trust level on the imported key. The signature is still good.*

gpg: Good signature from "Shaky>" [unknown]gpg:

WARNING: This key is not certified with a trusted signature! gpg: There is no indication that the signature belongs to the owner.

-----BEGIN PGP SIGNED MESSAGE----- Hash: SHA512

This is a test message from Shakybeats. If you have imported my key you will see a good signature on this message.

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEE/RMB93kpCo0FElYna7uXKSYEvL0FAl7fpyIACgkQa7uXKSYE
vL3MAg/+K4+Nce4QIUIbDRfyZwocRfiOb/585xuukCwCC01hb4QB2MW4nR6XC9aq
nkJ7PLm2XQ759suE3ntsohRt4jzHTa4v/EOPmv16h5TL0QOTCYJhAHyAiCR42nDW

ezEZBDEPrc3LUWDXo0MMxTOXkKcfqbZq2+s624OQ61KXTy8OFKjooGZo
DdV214kL

UKct+u0PQh6NVGS7kv+UtH6yq6XWj20QpgaHrMGMoe296Ub5Rz8xZ
eKdOQEV7aVr

hcfcmWizhrAB7mF2pFH6Wb97i1xerbSFeXE/yCxyEmvB2pHtOnIQnp
Hnwg6NEJxI
X+HbdqYlxkEB4nbbYnaAqH3TJnOf7zx5MzitRpAD3wJxpgsOHC3U7SjKA
TRoSlLX
ImRYo0FwL8OKMf7wmHFktK4V+HeTWype86TTKoYi+y/u1K/DW8Ngkw
n0HI7PpV3x

3YjCcnYsckvdjpbFYO/WPLd/ABaK/sVHEijP1jSEsP6yAZ/N4e9pSLf
DARh6sqNX
bzHIoXQXIKpzjtuxYwy/IJh5piac7VofXyT60rr2jQIv+nghzahwpzDJWOfC7y
XS
WQK//lxqaX2+JPOrNf+CN2CxBR/sX/Dx5jrgQoCgkKhDcQeSfjLHc3Oei9
glidPl
iahWsoXxBYBP1PukBdjvSWrTqJOWFoIyygTaMp1f8Y45roJd45k==FiRc
-----END PGP SIGNATURE-----

Verifying a onion address

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv-7jicoxknyazubrad.onion/post/c826a3b3dab5b671ec6d

Now that you know how to verify a signature we can verify an onion address. First we need to get a markets pgp key. Most markets put them on their subdread, but if not you can put /pgp.txt at the end of the mirror you want to verify. It should look like this: MarketOnionAddress.onion/pgp.txt

You'll probably have to complete a captcha. Then you should see the markets PGP key. Import the key like normal. (See above if you neeed help)

Once you have it imported put /mirrors.txt at the end of the onion you are on.

It should look something like this MarketOnionAddress.onion/mirrors.txt

***Note:** Some markets don't use mirrors.txt check their subdread for what you should put at the end to verify.*

After you do that you should see a signed PGP Signature (Like mine above) If you have the market pgp imported you should get a good signature from it. At the top you will see a list of the current market mirrors. Make sure the address you are on matches one of the ones in the signed message. If it does you are on a official market onion!

Once you do this a few times it really only takes about 15 seconds to do.

Note: Always take the time to verify an onion regardless of where you get them from

Do Look at your Tor Logs

From Firefox browser Settings about:preferences#tor

3/27/22, 21:37:06.109 [NOTICE] DisableNetwork is set. Tor will not make or accept non-control network connections. Shutting down all existing connections.

3/27/22, 21:37:06.138 [NOTICE] Opening Socks listener on 127.0.0.1:9150

3/27/22, 21:37:06.138 [NOTICE] Opened Socks listener connection (ready) on 127.0.0.1:9150

3/27/22, 21:37:06.271 [NOTICE] Application request when we haven't used client functionality lately. Optimistically trying directory fetches again.

3/27/22, 21:37:06.564 [NOTICE] Application request when we haven't used client functionality lately. Optimistically trying directory fetches again.

3/27/22, 21:37:06.564 [NOTICE] Application request when we haven't used client functionality lately. Optimistically trying directory fetches again.

3/27/22, 21:37:06.653 [NOTICE] Application request when we haven't used client functionality lately. Optimistically trying directory fetches again.

3/27/22, 21:37:06.653 [NOTICE] Application request when we haven't used client functionality lately. Optimistically trying directory fetches again.

3/27/22, 21:37:06.653 [NOTICE] Application request when we haven't used client functionality lately. Optimistically trying directory fetches again.

3/27/22, 21:37:07.674 [NOTICE] Bootstrapped 5% (conn): Connecting to a relay

3/27/22, 21:37:08.190 [NOTICE] Bootstrapped 10% (conn_done): Connected to a relay

3/27/22, 21:37:08.477 [NOTICE] Bootstrapped 14% (handshake): Handshaking with a relay

3/27/22, 21:37:09.118 [NOTICE] Bootstrapped 15% (handshake_done): Handshake with a relay done

3/27/22, 21:37:09.119 [NOTICE] Bootstrapped 20% (onehop_create): Establishing an encrypted directory connection

3/27/22, 21:37:09.274 [NOTICE] Bootstrapped 25% (requesting_status): Asking for networkstatus consensus

3/27/22, 21:37:09.427 [NOTICE] Bootstrapped 30% (loading_status): Loading networkstatus consensus

3/27/22, 21:37:11.510 [NOTICE] Bootstrapped 75% (enough_dirinfo): Loaded enough directory info to build circuits

3/27/22, 21:37:11.511 [NOTICE] Bootstrapped 90% (ap_handshake_done): Handshake finished with a relay to build circuits

3/27/22, 21:37:11.511 [NOTICE] Bootstrapped 95% (circuit_create): Establishing a Tor circuit

3/27/22, 21:37:12.423 [NOTICE] Bootstrapped 100% (done): Done

3/27/22, 21:37:31.710 [NOTICE] Your network connection speed appears to have changed. Resetting timeout to 60000ms after 18 timeouts and 168 buildtimes.

Being Safe on the Dark Web

It would be a dereliction for me not to impart to my readers some lessons learned and best practices from my adventures of Going Deep.

Truecrypt is an open source tool which can help you to encrypt your data and stay anonymous online. Truecrypt and Microsoft's BitLocker are powerful tools, for volume, partition, folder, file, and drive encryption You can also set up hidden volumes or a hidden OS.

https://www.zdnet.com/article/best-encryption-software/

https://www.pcmag.com/picks/the-best-encryption-software

BleachBit is one open source GNU licensed free software programs which can shred your files so as to prevent any recovery, and then overwrite your free disk space so as to hide the traces of the old files. The tool hunts down and then automatically deletes any unnecessary files located anywhere on the hard disk, from the caches and the cookies to temporary folders belonging to thousands of applications.

Keep Tor up to date. Shortly after Firefox updates, which are frequent, there will be a Tor update.

Hide your network card MAC address (serial number) In Windows click on the Advanced tab and then choose Network Address from the list. If you do not find this feature, just know that your network adapter is not capable of supporting this. Enable the value, and then type in the MAC address which you desire. Ensure that you don't use any characters such as colons for colons. Click Ok and you are done.

If that does not work, because you do not see the Network Address item, try this:

Spoofing your MAC address (network card serial number)

At a command prompt use the getmac command or use ipconfig /all to discover it.

Use Technetium MAC Address Changer | A Freeware Utility

https://technitium.com/tmac/

https://blog.technitium.com/2011/05/tmac-issue-with-wireless-network.html

More Tips:

No More Java, JavaScript, and Flash, too leaky.

Note: PGP Tools requires Java to be installed.

No More Peer-to-Peer, no sharing.

Be a Cookie Monster, kill browser cookies.

Use Fake email Accounts when you can.

Use email that requires Tor.

Bye, Bye Google use Duckduckgo or StartPage for no data collection.

Act Legally, pretend your Mom is watching you.

Use bookmarks to avoid bad sites, onion address change frequently.

Do not run a Tor onion site server from your home, unless you want the Feds to end up owning it and all your equipment.

The TLA's; NSA, CIA, and FBI, oh my!

Sources:

Rowley, William. How to Stay Anonymous on the Internet: Disappearing from the Web.

Jones, Jack. The Complete Beginners Guide To Tor, & Accessing The Dark Web, Deep Net, Dark Net).

Firefox Rolls Out Total Cookie Protection By Default To All Users Worldwide

Posted by msmash on Tuesday June 14, 2022 @11:00AM from the moving-forward dept.

Mozilla:

Starting today, Firefox is rolling out Total Cookie Protection by default to all Firefox users worldwide, making Firefox the most private and secure major browser available across Windows and Mac. Total Cookie Protection is Firefox's strongest privacy protection to date, confining cookies to the site where they were created, thus preventing tracking companies from using these cookies to track your browsing from site to site. Whether it's applying for a student loan, seeking treatment or advice through a health site, or browsing an online dating app, massive amounts of your personal information is online -- and this data is leaking all over the web.

The hyper-specific-to-you ads you so often see online are made possible by cookies that are used to track your behavior across sites and build an extremely sophisticated profile of who you are. Recent stories (including an excellent Last Week Tonight episode) have shown how robust, yet under-the-radar, the data selling economy is and how easy it is for anyone to buy your data, combine it with more data about you and use it for a variety of purposes, even beyond advertising. It's an alarming reality -- the possibility that your every move online is being watched, tracked and shared -- and one that's antithetical to the open web we at Mozilla have strived to build. That's why we

developed Total Cookie Protection to help keep you safe online.

Total Cookie Protection works by creating a separate "cookie jar" for each website you visit. Instead of allowing trackers to link up your behavior on multiple sites, they just get to see behavior on individual sites. Any time a website, or third-party content embedded in a website, deposits a cookie in your browser, that cookie is confined to the cookie jar assigned to only that website. No other websites can reach into the cookie jars that don't belong to them and find out what the other websites' cookies know about you -- giving you freedom from invasive ads and reducing the amount of information companies gather about you. This approach strikes the balance between eliminating the worst privacy properties of third-party cookies -- in particular the ability to track you -- and allowing those cookies to fulfill their less invasive use cases (e.g. to provide accurate analytics). With Total Cookie Protection in Firefox, people can enjoy better privacy and have the great browsing experience they've come to expect.

Browser Fingerprinting

(Aka A Violation of Your Privacy)

Definition:

A device fingerprint or machine fingerprint is information collected about the software and hardware of a remote computing device for the purpose of identification. The information is usually assimilated into a brief identifier using a fingerprinting algorithm. A browser fingerprint is information collected specifically by interaction with the web browser of the device.

Device fingerprints can be used to fully or partially identify individual devices even when persistent cookies (and zombie cookies) cannot be read or stored in the browser, the client IP address is hidden, or one switches to another browser on the same device. This may allow a service provider to detect and prevent identity theft and credit card fraud, but also to compile long-term records of individuals' browsing histories (and deliver targeted advertising) or targeted exploits even when they are attempting to avoid tracking – raising a major concern for Internet privacy advocates.

https://en.wikipedia.org/wiki/Device_fingerprint

How does online fingerprint identify me?

With browser fingerprints, the information collected about you includes numerous data points that predominantly help track the following details.

Type of browser and version
Browser settings
Active plugins
IP address
Device Operating System
Device type and model

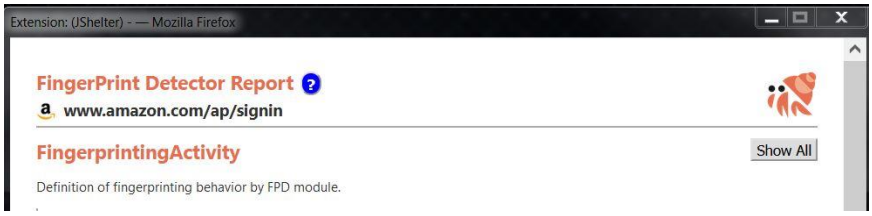
Network type (or ISP)
Device time zone
Users' location
Language
Screen resolution
Active JavaScript
Active Flash

Example: Firefox 100.02 (64-bit)

Use Firefox JShelter JavaScript shield to prevent fingerprinting

FingerPrint Detector Report

This report lists all JavaScript API endpoints that were accessed by the web page and are considered critical in terms of browser fingerprinting. Fingerprint Detector (FPD) uses this data to decide whether the page is collecting a browser fingerprint.



FPD processes API calls in groups based on their semantic properties. This window shows the detected number of API calls9 on the visited page. The default view shows only groups accessed at least once.

FingerprintingActivity
Definition of fingerprinting behavior by FPD module.
BrowserProperties
Fingerprinting methods based on simple information gathering by

[9] *An application-programming interface (API) is a connection between computers or between computer programs. It is a type of software interface, offering a service to other pieces of software. A document or standard that describes how to build or use such a connection or interface is called an API specification. A computer system that meets this standard is said to implement or expose an API. The term API may refer either to the specification or to the implementation.* https://en.wikipedia.org/wiki/API

accessing certain APIs.
- MediaDevices.prototype.enumerateDevices (1)
- HTMLMediaElement.prototype.canPlayType (34)
NavigatorBasic
Basic information about browser and system.
- Navigator.prototype.userAgent (53)
- Navigator.prototype.platform (3)
- Navigator.prototype.productSub (1)
- Navigator.prototype.product (13)
- Navigator.prototype.vendorSub (1)
- Navigator.prototype.vendor (1)
- Navigator.prototype.appVersion (1)
- Navigator.prototype.appCodeName (1)
NavigatorHardware
Hardware information about device.
- Navigator.prototype.hardwareConcurrency (1)
NavigatorMobile
Information about features supported by mobile devices.
- Navigator.prototype.maxTouchPoints (1)
ScreenInfo
Information about screen and its properties.
- Screen.prototype.height (1)
- Screen.prototype.width (1)
- Screen.prototype.colorDepth (1)
- Screen.prototype.pixelDepth (1)
- Screen.prototype.availHeight (1)
- Screen.prototype.availWidth (1)
WindowInfo
Information about screen from root Window object.
- window.devicePixelRatio (5)
- window.innerWidth (14)
- window.innerHeight (16)
- window.outerWidth (1)
- window.outerHeight (1)
StorageInfo
Availability of WebStorage technology.
- window.localStorage (65)
- window.sessionStorage (18)
- window.indexedDB (3)
NavigatorFlags
Binary browser settings.
- Navigator.prototype.doNotTrack (1)
TimeInfo
Information about exact time values.
- Performance.prototype.now (59)
- Date.now (1000+)
WebGLInfo
Information from WebGL/WebGL2 interface.
- WebGLRenderingContext.prototype.getParameter (26)
AlgorithmicMethods

Fingerprinting methods based on specific procedures, calculations or processing.

FontsEnumFingerprint
System fonts enumeration techniques.
- CSSStyleDeclaration.prototype.fontFamily (n/a)
- HTMLElement.prototype.offsetWidth (3)
- HTMLElement.prototype.offsetHeight (8)
- CanvasRenderingContext2D.prototype.font (83)
- CanvasRenderingContext2D.prototype.measureText (73)
CanvasFingerprint
Extraction of rendered image from 2D canvas.
- CanvasRenderingContext2D.prototype.fillText (10)
- CanvasRenderingContext2D.prototype.fillStyle (11)
- HTMLCanvasElement.prototype.toDataURL (5)
- CanvasRenderingContext2D.prototype.getImageData (21)
WebGLFingerprint
Extraction of rendered image from WebGL canvas.
- HTMLCanvasElement.prototype.toDataURL (5)
- CanvasRenderingContext2D.prototype.getImageData (21)
- HTMLCanvasElement.prototype.toDataURL (5)
- CanvasRenderingContext2D.prototype.getImageData (21)
WebRTCFingerprint
Leakage of public or local IP address.
- RTCPeerConnection.prototype.createDataChannel (1)
- RTCPeerConnection.prototype.createOffer (1)
CrawlFpInspector
APIs often abused for fingerprinting according to FP-Inspector study.
- Navigator.prototype.productSub (1)
- Navigator.prototype.vendorSub (1)
- Navigator.prototype.appCodeName (1)
- Navigator.prototype.hardwareConcurrency (1)
- Navigator.prototype.maxTouchPoints (1)
- Navigator.prototype.doNotTrack (1)
- MediaDevices.prototype.enumerateDevices (1)
- WebGLRenderingContext.prototype.getParameter (26)
- CanvasRenderingContext2D.prototype.fillStyle (11)
- HTMLCanvasElement.prototype.toDataURL (5)
- CanvasRenderingContext2D.prototype.getImageData (21)
- WebGLRenderingContext.prototype.getExtension (2)
- Navigator.prototype.buildID (1)
WebGLRenderingContext.prototype.getSupportedExtensions (1)
- Navigator.prototype.oscpu (1)
- WebGLRenderingContext.prototype.getContextAttributes (1)
WebGLRenderingContext.prototype.getShaderPrecisionFormat (12)
- WebGLShaderPrecisionFormat.prototype.rangeMax (12)
- CanvasRenderingContext2D.prototype.textBaseline (2)
- CanvasRenderingContext2D.prototype.fillRect (2)
- CanvasRenderingContext2D.prototype.beginPath (1)

These data collections are corporate decisions made to harvest this data from unsuspecting website visitors. This is just more of the current corporate vulture capitalism at work, as if a giant squid wrapped itself around the Internet, sticking its tentacles into anything and everything to suck out, harvest, and process any and all information that they can somehow turn into money.

Some people block their browser cookies, so they respond in turn by doing this fingerprinting. No one consensually agreed, nor were asked to allow this kind of unsolicited and unremunerated privacy intrusion.

The Firefox web browser warns you about this. Apple Safari, Microsoft Edge, and Google Chrome will not because they are part of the problem. If you turn off JavaScript[10] and Flash, and add a privacy browser extension, you may be able to thwart these privacy intrusions with these corporate browsers.

There is very good information and advice on this here:

https://privacysavvy.com

https://privacysavvy.com/security/safe-browsing/browser-fingerprinting/

Tor Browser results

Our tests indicate that you have you have strong protection against Web tracking, though your software isn't checking for Do Not Track policies.
IS YOUR BROWSER:
Blocking tracking ads? Yes
Blocking invisible trackers? Yes
Protecting you from fingerprinting? Yes

This is what your test should look like.

https://www.wikihow.com/Disable-JavaScript

Notes:

1. **You cannot disable JavaScript in the iPhone or iPad version of Firefox.**
2. **You cannot disable JavaScript in the iPhone or iPad version of Chrome.**
3. **When you update Google Chrome, you may have to re-disable JavaScript.**

---

[10] *This may cause problems with lots of websites, so bookmark your preferences page in your browser, i.e. in Firefox about:config.*

4. **You may have to re-disable JavaScript after you update your iPhone.**
5. **When you update the Firefox app, you may need to disable JavaScript again.**

And all of this tells you somethings right there.

Note: Disabling JavaScript is also a quick way to load content-rich websites when on a slow Internet connection.

To Dark Web Search

Finding and navigating your way through the Dark Web bits and bytes

All onion Dark Web sites now use a16 character URL (universal resource locator) ending in (dot) .onion (rather than dot gov, dot org, dot edu, dot net, dot io, dot com or hundreds of country codes. There is no DNS[11] translation needed from domain names like cnn.com that people understand, to and IP address of 151.101.193.67 that computers understand.

Important Update: Onion v3 is Here

Onion website URLs have now changed due to a shift towards the v3 protocol.

That means many of the existing websites will no longer be accessible unless you know the new v3 .onion address.

There are various reasons for the change, including better code and improved security.

To see if the URL you are trying to access is v2 or v3, the most telling sign is the length of the URL. v3 .onion addresses are 56 characters in length. The older v2 URLs are only 16 characters in length.

Getting to know new v3 .Onion URLs is very important as Tor client updates in October 2021 rendered all v2 addresses obsolete.

A sample v2 .onion link:

http://hss3uro2hsxfogfq.onion

---

[11] The Domain Name System (DNS) is the hierarchical and decentralized naming system used to identify computers reachable through the Internet or other Internet Protocol (IP) networks.

https://en.wikipedia.org/wiki/Domain_Name_System

A sample v3 .onion link:

http://eludemailxhnqzfmxehy3bk5guyhlxbunfyhkcksv-4gvx6d3wcf6smad.onion/

Search Sites

Ahmia

http://juhanurmihxlp77nkq76byazcldy2hlmovfu-2epvl5ankdibsot4csyd.onion/

This search engine's mission is to be leaders in providing services on the Deep Web, protecting the anonymity of each user. In addition, they share information of great importance, about the Tor network and the Tor project.

Ahmia developers believe that the Tor network is an important distributed platform to protect anonymity and privacy around the world. However, by providing a search engine for what many call the "deep network" or "dark network," Ahmia makes hidden services accessible to a wide range of people, not just early adopters of the Tor network. .

The "Ahmia" search system is integrated with "GlobaLeaks." That it is an open source project that is in charge of handling suggestions and comments anonymously. On the other hand, we have Tor2Web, which is a service that helps people who are not yet in the Tor network.

Beginning in September 2013, "Ahmia" has been affiliated with the "Hermes Center," for digital transparency. This is an organization dedicated to developing and promoting the transparency of technologies that allow freedom around the world.

Ahmia's mission is to create the premier search engine for services residing on the Tor anonymity network. In doing so, we hope to share meaningful statistics, insights, and news about the Tor network and the Tor project.

Contributors to Ahmia believe that the Tor network is an important and resilient distributed platform for anonymity and privacy worldwide. By providing a search engine for what many call the "deep web" or "dark net", Ahmia makes onion services accessible to a wide range of people, not just Tor network early adopters.

Juha Nurmi (juha.nurmi@ahmia.fi) (Finland) is the founder and project leader of the Ahmia search engine project. He is a security researcher, and has been involved in numerous projects funded by both the commercial and government spheres. Juha is also a noted lecturer and public speaker.

Ahmia is an active area of research, and is in development on GitHub as a free and open source project.

Ahmia searches hidden services on the Tor network. To access these hidden services, you need the Tor browser bundle. Abuse material is not allowed on Ahmia. See our service blacklist and report abuse material if you find it in the index. It will be removed as soon as possible.

For more about Ahmia, see indexing information , contribute to the source code.

The Tor Project Onion service: juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion

HiddenWiki

http://zqktlwi4fecvo6ri.onion-/wiki/index.php/Main_Page

The Hidden Wiki is the collection of the most popular Dark Web links & services. Also includes FAQs on Dark Web.

main page
discussion
view source
history
The Hidden Wiki
Main Page
Welcome to The Hidden Wiki! Our official Hidden Wiki url in 2022 is:
http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion
Add it to bookmarks and spread it!!!!
navigation
Main page
Recent changes
Random page
Rules of the site
search
Search The Hidden Wiki
Go
Search
Editor's picks
Pick a random page from the article index and replace one of these slots with it:
1. The Matrix - Very nice to read.
2. How to Exit the Matrix - Learn how to Protect yourself and your rights, online and off.
3. Verifying PGP signatures - A short and simple how-to guide.
4. In Praise Of Hawala - Anonymous informal value transfer system.
5. Terrific Strategies To Apply A Social media Marketing Approach - Great tips for the internet marketer

Our official Hidden Wiki URL in 2022 is:

http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym-2qad.onion

OnionLinks

http://s4k4ceiapwwgcm3mkb6e4diqecpo7kvdnfr-5gg7sph7jjppqkvwwqtyd.onion/

This is a categorized list of notable onion services (formerly, hidden services) accessible through the Tor anonymity network.

- **Financial Services**
- **Commercial Services**
- **Drugs**
- **Chans**
- **Privacy Services**
- **Email Providers**
- **Blogs and Personal Sites**
- **Hacking**
- **News Sites**
- **Open Source Software**

https://en.wikipedia.org/wiki/List_of_Tor_onion_services#Search_engines

Duckduckgo

DuckDuckGo – For the DarkNet, but searches only the Clearnet.

https://duckduckgogg42xjoc-72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/

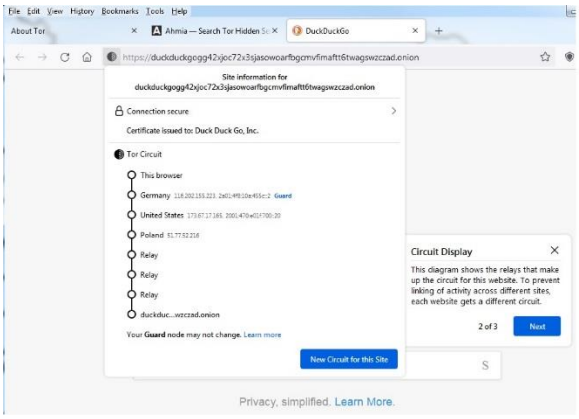
https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt-6twagswzczad.onion/html/–

Some reasons why you should not necessarily trust DuckDuckGo on the Dark Web

- **It is hosted on Amazon Web Services (which has a $600 million contract with the CIA)**
- **Gabriel Weinberg, the creator and owner formerly ran a site called NamesDatabase which encouraged people to provide valid personal details and to refer other people to give their information**
- **They save searches, but again, not in a personally identifiable way, as we do not store IP addresses or unique User agent strings. We use aggregate, non-personal search data to improve things like misspellings."**
- **Despite bangs simply referring to another search engine, "Bang" queries are still send to and stored by DuckDuckGo (this could be solved with Javascript is enabled, or in one of its extensions/apps)**
- **DuckDuckGo knows whether you are scrolling down on the page since website icons are lazy loaded**
- **On the Hidden Service website icons are still fetched from duckduckgo.com**
- **DNS registration information is protected by WhoisGuard**
- **Google has released the Duck.com domain name for DuckDuckGo in 2018**
- **Apple (in 2014) and Mozilla (in 2018) have added DuckDuckGo as a search engine option**
- **DuckDuckGo used to set cookies even though they said they did not**

- **DuckDuckGo used to submit the URL you are clicking on to DuckDuckGo's servers**

  https://duckduckgo.com/privacy
  http://www.alexanderhanff.com/duckduckgone


File Edit View History Bookmarks Tools Help
About Tor
Ahmia — Search Tor Hidden
DuckDuckGo
Site information for
Connection secure
Certificate issued to: Duck Duck Go, Inc.
Tor Circuit
This browser
Germany
United States
Poland
Relay
Relay
Relay
Your Guard node may not change. Learn more
New Circuit for this Site
Circuit Display
This diagram shows the relays that make up the circuit for this website. To prevent linking of activity across different sites, each website gets a different circuit.
2 of 3
Next
Privacy, simplified. Learn More.

The Tor circuit paths, note the beginning, middle, and exit relay sites.

Bing Contract Prohibits DuckDuckGo From Completely Blocking Microsoft Tracking (reviewgeek.com) 58

Posted by BeauHD on Tuesday May 24, 2022 from the deal-with-the-devil dept.

DuckDuckGo isn't as private as you thought. "Due to a confidential search agreement, the DuckDuckGo browser does not block all Microsoft trackers," reports Review Geek. "What's worse, DuckDuckGo only acknowledged this 'privacy hole' after it was discovered by a security researcher." From the report: Security researcher @thezedwards *found that the mobile DuckDuckGo browser does not block Microsoft trackers on third-party websites, such as the Facebook-owned Workplace.com. Gabriel Weinberg, the CEO of DuckDuckGo, is now running damage control on Twitter. He explains that Microsoft cannot see what you search in DuckDuckGo, and the DuckDuckGo browser blocks all Microsoft cookies. But if you visit a website that contains Microsoft's trackers, then your data is exposed to services like Bing and LinkedIn. This is the result of DuckDuckGo's "search syndication agreement" with Microsoft. In order to pull search information from Bing, the privacy experts at DuckDuckGo have to poke holes in their browser's security system.*

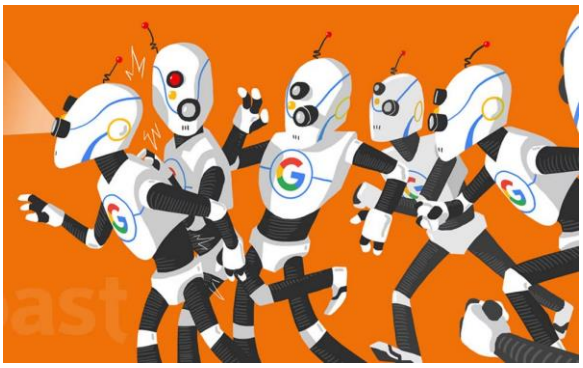
While DuckDuckGo has a solid privacy policy when it comes to Microsoft's ads*, it hasn't explained how Microsoft uses data from third-party trackers. And that's quite alarming. Maybe this situation is overblown, or maybe Microsoft can build targeted ad profiles based on your web activity in DuckDuckGo -- we don't know because DuckDuckGo signed a confidentiality agreement. Gabriel Weinberg says that DuckDuckGo is "*working tirelessly behind the scenes*" to improve its deal with Microsoft. Additionally, he expects DuckDuckGo to "include more third-party Microsoft protection" in a future update.*

Why is the Deep Web not indexable?

Several methods prevent web pages from being indexed by traditional search engines.

- **Contextual Web:** Pages with content varying for different access contexts.
- **Dynamic content:** Dynamic pages which are returned in response to a submitted query or accessed only through a form, especially if open-domain input elements are used; such fields are hard to navigate without domain knowledge.
- **Limited access content:** Sites that limit access to their pages in a technical way (e.g., using the Robots Exclusion Standard or CAPTCHAs, or no-store directive which prohibit search engines from browsing them and creating cached copies).
- **Non-HTML/text content:** Textual content encoded in multimedia (image or video) files or specific file formats not handled by search engines.
- **Private Web:** Sites that require registration and login (password-protected resources).
- **Scripted content:** Pages that are only accessible through links produced by JavaScript as well as content dynamically downloaded from Web servers via Flash or Ajax solutions.
- **Software:** Certain content is intentionally hidden from the regular Internet, accessible only with special software, such as Tor, I2P, or other DarkNet software. For example, Tor allows users to access websites using the .onion server address anonymously, hiding their IP address.
- **Unlinked content:** Pages which are not linked to by other pages, which may prevent Web crawling programs from accessing the content. This content is referred to as pages without backlinks (also known as inlinks). Also, search engines do not always detect all backlinks from searched web pages.
- **Web archives:** Web archival services such as the Wayback Machine enable users to see archived versions of web pages across time, including websites which have become inaccessible, and are not indexed by search engines such as Google.

https://en.wikipedia.org/wiki/Deep_web



You can Stop the Bots!

A few alternatives:

Searx

https://github.com/asciimoo/searx/wiki/Searx-instances

Qwant

https://www.qwant.com/

StartPage

https://www.startpage.com/

http://hss3uro2hsxfogfq.onion – not Evil – The premier search engine of onionland.

http://visitorfi5kl7q7i.onion – visitor – Evil and clone domains filtered. Good accuracy.

http://msydqstlz2kzerdg.onion – Ahmia.fi – onion and tor2web search links. Reasonable accuracy.

http://xmh57jrzrnw6insl.onion – Torch – onion searches. Poor search-result accuracy.

http://7pwy57iklvt6lyhe.onion – Dark Search Enginer - A new search engine for the DarkNet.

http://bznjtqphs2lp4xdd.onion – Dark Web links – A new search engine. Poor result accuracy.

http://searchb5a7tmimez.onion – searx – Search engine for the Clearnet. Categories.

http://gjobqjj7wyczbqie.onion – Candle – Retro-like-design. Fine search-result accuracy.

http://kbhpodhnfxl3clb4.onion – TorSearch – Around 410K .onion pages indexed currently.

http://carontevaha5x626.onion – Caronte – A new search engine with good accuracy.

Software tools to make the Dark Web more transparent are constantly evolving, as is the software criminals use to hide their activity. Government agencies and law enforcement can now use Memex[12], a search engine developed by DARPA and designed specifically for the Dark Web, to find sites and store data that can be analyzed later. A number of United States federal agencies use Memex in counter-terrorism. As originally theorized, Memex was a machine that could act as an extension to the human memory, into which vast amounts of varied information could be deposited and later retrieved. Wikipedia

The US government making use of this name is seen by some as an evil perversion of the original idea.

[12] *The individual person was intended to use the Memex as an automatic personal filing system, making the Memex "an enlarged intimate supplement to his memory" to advance human thinking. The name Memex is a portmanteau of memory and expansion. The idea came from Vannevar Bush in 1945.*

Scientia est potential or knowledge is power.[13]

NSA Says 'No Backdoor' for Spies in New US Encryption Scheme (bloomberg.com) 29

Posted by msmash on Friday May 13, 2022 @10:10AM from the sure,-jan dept.

The US is readying new encryption standards that will be so ironclad that even the nation's top code-cracking agency says it won't be able to bypass them. From a report: The National Security Agency has been involved in parts of the process but insists it has no way of bypassing the new standards. "There are no backdoors," said Rob Joyce, the NSA's director of cybersecurity at the National Security Agency, in an interview. A backdoor enables someone to exploit a deliberate, hidden flaw to break encryption. An encryption algorithm developed by the NSA was dropped as a federal standard in 2014 amid concerns that it contained a backdoor. The new standards are intended to withstand quantum computing, a developing technology that is expected to be able to solve math problems that today's computers can't. But it's also one that the White House fears could allow the encrypted data that girds the U.S. economy -- and national security secrets -- to be hacked.

The government lie? Not possible?

Clapper took over in 2010 heading up 17 different intelligence agencies. His tenure was marked by the Edward Snowden leaks on US intelligence.

"NOT WITTINGLY" – JAMES CLAPPER

Remember the famous moment when US NATIONAL INTELLIGENCE CHIEF James Clapper was testifying about the NSA surveillance of Americans when he let slip a sign he was not being truthful. Of course, we knew this was all a smoke and mirrors show. Clapper later said he "misspoke"…last we checked it's pretty much the same thing as lying…

---

[13] *The phrase "scientia est potentia" is a Latin aphorism meaning "knowledge is power". It is commonly attributed to Sir Francis Bacon. Wikipedia*

A revelations from Edward Snowden's Leaks

Secret court orders allow NSA to sweep up Americans' phone records

Verizon had been providing the NSA with virtually all of its customers' phone records. It soon was revealed that it was not just Verizon, but also virtually every other telephone company in America.

Things That Happened Because Of The NSA Leaks

Director of National Intelligence James Clapper had to admit he lied to Congress. "I gave the least untruthful answer."

Three months before the Snowden leaks began; Sen. Ron Wyden (D-Ore.) asked the nation's top intelligence official if the NSA collected data on millions, or hundreds of millions, of Americans.

"No, sir," Clapper replied. "Not wittingly."

By that point, of course, the NSA had quite wittingly been running a massive bulk telephone metadata collection program for years. The government had repeatedly asked a secret surveillance court for permission to do so, and it deemed every American's phone record "relevant" to terrorism in the process.

Wyden fumed in secret about Clapper's lie — but felt he could not reveal it because the metadata collection program was classified. That all changed after the publication of the first story on June 5, 2013, based off a Snowden leak.

Days later, Clapper gave the most halfhearted, or perhaps least forthcoming, admission that he had lied: "I responded in what I thought was the most truthful or least untruthful manner by saying no."

The House of Representatives then passed a bill (ostensibly) meant to stop bulk collection of phone metadata.

Snowden also revealed NSA efforts to crack encryption and undermine Internet security

Encryption makes data flowing through the Internet unreadable to hackers and spies, making the NSA's surveillance programs less useful. What is the point of tapping fiber optic cables if the data flowing through them is unreadable? That is why the NSA has a developed a series of techniques and tricks to circumvent widely used web encryption technologies.

Onion Search Engine

Has a language translate function.

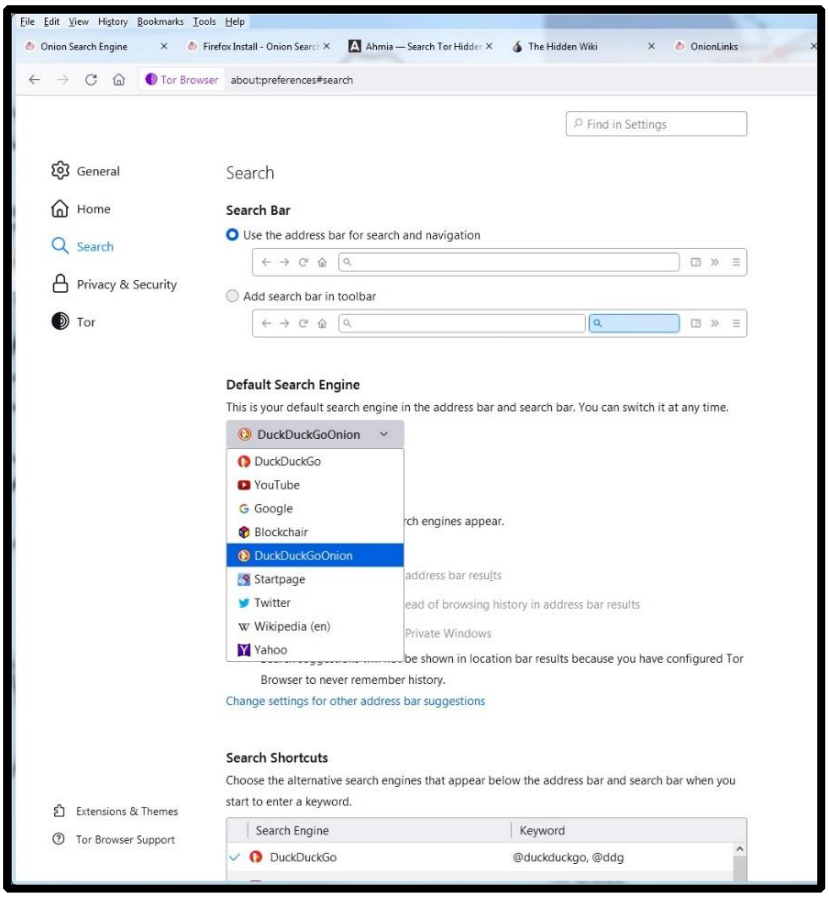
http://zgphrnyp45suenks3jcscwvc5zllyk3vz4izzw-67puwlzabw-4wvwufid.onion/

Onion Search Engine
"No cookies, no javascript, no trace. We protect your privacy"
* Onion service: Hidden 1, Hidden 2
NEWS
Onion Network
Standard Network
Add Onion Search Engine to Firefox

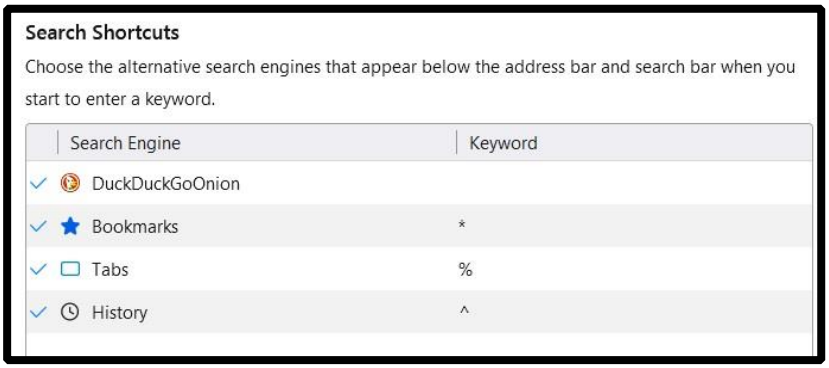
TorDex

http://tordexpmg4xy32rfp4ovnz7zq5ujoejwq-2u26uxxtkscgo5u3losmeid.onion/

Pick your search engine in Tor



Tor Search Settings



Tor Search Shortcuts

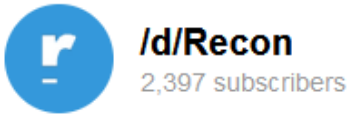
HayStak

HayStak is a Dark Web search engine started by a group of privacy campaigners who believe the Internet should be free from state surveillance. To date HayStak has indexed 1.5 billion pages over 260,000 .onion websites.

http://haystak5njsmn2hqkewecpaxetahtwhsbsa-64jom2k22z5afxhnpxfid.onion/

haystak: your darknet search engine
enter your query here
Search
224640 searches performed today on the darknet's largest search engine. We've indexed 1.5 billion pages over 260,000 onions (including historical onions)
Please help us run haystak for free by donating to 1Ko21k9yXewTTF77QGk8crXarFFC9o37z4, all donations greatfully received.

Recon Search Site

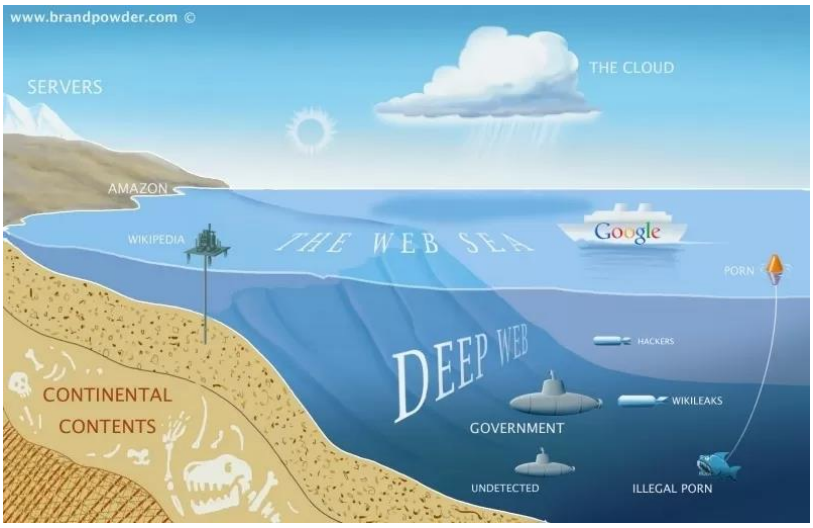


http://recon222tttn4ob7ujdhbn3s4gjre7netvzybuvbq-2bcqwltkiqinhad.onion/

Compare products from every market with the most powerful Dark Net Market search engine.

/d/Recon sub on dread

http://dreadytofatroptsdj6io7l3xptbet6onoyno-2yv7jicoxknyazubrad.onion/d/Recon



Deeplink Onion Directory

http://deeeepv4bfndyatwkdzeciebqcwwlvgqa-6mofdtsvwpon4elfut7lfqd.onion/

DeepLink Onion Directory
Home Add Site Contact
Western Union
Hacked Bitcoin Wallets
ONION LINKS TORNODE DIRECTORY
Hacked Bitcoin Wallets
WU TRANSFER
Paul Links | Verified & Safe
DEEP
Open your store for FREE CLICK HERE
Links CLICK HERE
We don't send any email asking for money! any email pretend to be from us is SCAM !
DeepLink is moving to Onion-Version 3 Address: Please be sure to bookmark the right address!
http://deeeepv4bfndyatwkdzeciebqcwwlvgqa6mofdtsvwpon4elfut7lfqd.onion/
Search... Search
Categories:
All Onions
Market
Hacking
Hosting
Forums
Blog
Link List / Wiki
Communication
Social
Financial Services
Adult
Search Engines
Hidden Answers
Hidden questions and answers
http://answerh4rfo4zgi4ao7lzoukjflpbur4ldabarachwwhabbu4vkpvxyd.onion
368,180 25 7 5 V3 Status:Up and Running
PasteBox
PasteBox is a simple Tool to share your text.PasteBox never delete or censor a paste, except C-P . We do not have any filters enabled.
http://pasteboxx44wtzbm3ldjkcncls6uggi7mipmdwef5zza6wjqrqrtxdid.onion
90,351 15 0 0 V3 Status:Up and Running
CORE FORUM - 2021
Former admin/mod decided to create the best new forum. CORE
http://ksn5nqaie4bozit34yk5dnlxhdymd2fvusltutotvkamr5mv4ldkmgzqd.onion
251,952 7 1 3 V3 Status:Up and Running
DarkWebFrench
Forum Français non censuré sans limite. L'un des plus populaires
http://frenchwltobamdhyq5y2egezkbnz53ws5kaa6wnscildhnegdw5nhsyd.onion
234,622 5 0 0 V3 Status:Up and Running

Clear Web crawlers (spiderbots)

A Web crawler, sometimes called a spider or spiderbot and often shortened to crawler, is an Internet bot that systematically browses the World Wide Web and that is typically operated by search engines for the purpose of Web indexing (web spidering).

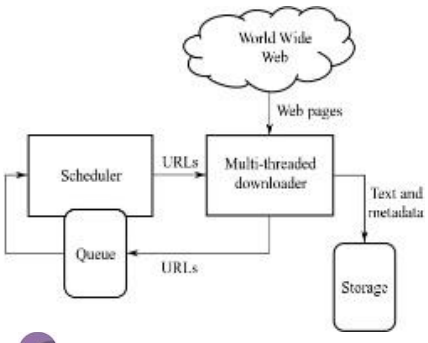
Web search engines and some other websites use Web crawling or spidering software to update their web content or indices of other sites' web content. Web crawlers copy pages for processing by a search engine, which indexes the downloaded pages so that users can search more efficiently.

Crawlers consume resources on visited systems and often visit sites unprompted. Issues of schedule, load, and "politeness" come into play when large collections of pages are accessed. Mechanisms exist for public sites not wishing to be crawled to make this known to the crawling agent. For example, including a robots.txt file[14] can request bots to index only parts of a website, or nothing at all.

The number of Internet pages is extremely large; even the largest crawlers fall short of making a complete index. For this reason, search engines struggled to give relevant search results in the early years of the World Wide Web, before the year 2000. Today, relevant results are given almost instantly.

Crawlers can validate hyperlinks and HTML code. They can also be used for web scraping and data-driven programming.

https://en.wikipedia.org/wiki/Web_crawler



https://www.robotstxt.org/

https://commons.wikimedia.org/w/index.php?curid=3374592

---

[14] *Web Robots (also known as Web Wanderers, Crawlers, or Spiders), are programs that traverse the Web automatically. Search engines use them to index the web content, spammers use them to scan for email addresses, and they have many other uses.*

Dark Web crawlers (spiderbots)

Search engines use crawlers to index the Dark Web, only.

Examples:

- Ahmia-index

Index containing onions crawled by your crawlers

- Ahmia-crawler

Crawls onions on the Tor network and feeds it to the index

dread Forum discussion on bots and counter bots
(It does have a spell checker believe it or not.)

The discourse here can be high schoolish in tone, syntax, and spelling, which is common in certain circles among those who believe this attention to detail to be only for the elites. Stupidity viewed as a superpower.

dread content everyware on the clear net .

by /u/AANVOER • 3 days ago in /d/Dread

/u/paris I check now and then the clear net for my username

and again there are new copys off dread darknet.markets

https://darknet.markets

https://cafedread.com

now al my content is all over the clear net can you plz explane to me why this is ?

it is indexing on the fly even deleted messages are all there on the clear net

/u/Paris A

Why? Because Dread is a website on the DarkNet which can be requested from by a computer. We do have preventions in place to counter bots but if they go the slow and steady route with a lot of different endgame sessions there is little we can do about it. This is the reason why we don't have full post deletion on dread when it comes to account deletion. Because it's pointless. If it's posted

publicly it can be archived and referenced to later on even if it's deleted on dread.

/u/linkpin is the community member who created and runs https://cafedread.com. It's mostly for archive purposes (in the case dread goes down). They have dread support to operate. There is no posting and it's read only.

Reply /u/AANVOER

again proof that /u/hugbunter whas fucking insain the good way becouse I dont think that the clearnet domain dark.markets had any chance if he was still around not a chance .....

Reply /u/Endless1

Should the search be public? Idk

Reply /u/DNMcunt

Assume everything you write here is being analysed and recorded. Take your own precautions. Use fresh accounts regularyly and use your private key to prove your identity as needed. Or find a new hobby stupid ass.

Reply /u/razpootin

Its not like its so damn difficult to come on here and read everything you write. Get a normal job if you're that paranoid. If there are any links to your username and real identity then you fucked up long ago, mate.

Reply /u/gumdrop

"help my posts on an easily accessible and open forum are being seen by others" lol what

Reply /u/bruh1234550

I mean it's pretty obvious that it would happen..? It's possible to archive basically any site with enough effort, so one of the most popular darknet forums is definitely going to be archived. If you used a little bit of logic and opsec, that shouldn't be an issue no matter what, but you just don't seem to care enough to do a tiny bit of research. As Paris says, the clearnet cafedread site is publicly run by a linkpin, and I feel like it's a pretty commonly known fact on this site.

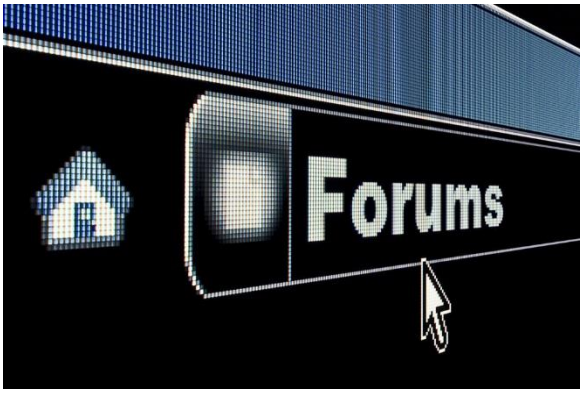
Reply /u/atmos

bro its a forum lol

/u/saturnmartin

I don't know why you would even care... dread is just as accessible as the clear-net, just free... Don't think this is the land of privacy. This is just the free Internet. If you want privacy improve your OpSec. Plus, it's great that we can access dread from the clear-net.

Dark Web Forums



Not everything on the Dark Web is evil because it was first utilized by journalists, whistleblowers, and human rights activists in oppressive regimes, as was its intended purpose.

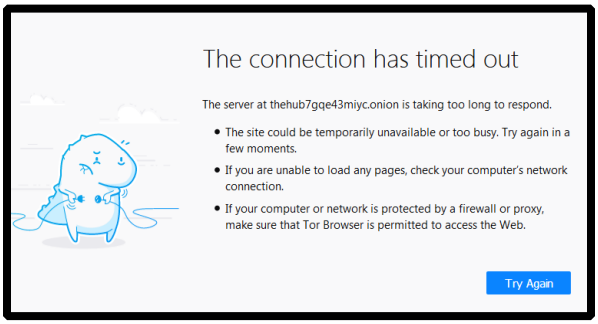
That said, there has always been a darker element, such as drug trafficking, gun trafficking, people trafficking, compromised data, such as bank account and credit card numbers, as well as stolen items..

Note: This book will not cover the dark markets, criminal activities, or the transactional side of the DW in this book.

But here is a list however:
https://darkweblink.com/top-darknet-markets-2022/

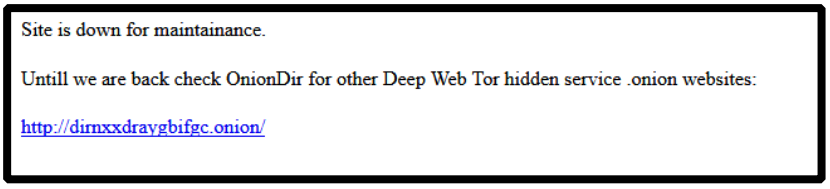
There are many lists of hidden dot onion links to be found, and much like the Clear Web circa 1995, many of these are dead links.

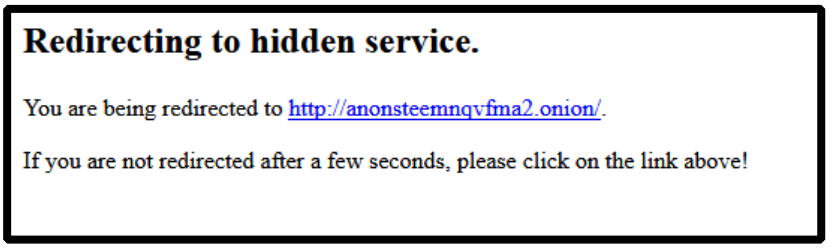
Note: In a recent analysis of the Dark Web by Securelist, many of these sites had a short lifespan. Most dark web sites were active for at least 200 days, but usually not more than 300 days. Some were online for less than two months.


The connection has timed out
The server at thehub7gqe43miyc.onion is taking too long to respond.
The site could be temporarily unavailable or too busy. Try again in a few moments.
If you are unable to load any pages, check your computer's network connection.
If your computer or network is protected by a firewall or proxy, make sure that Tor Browser is permitted to access the Web.
Try Again

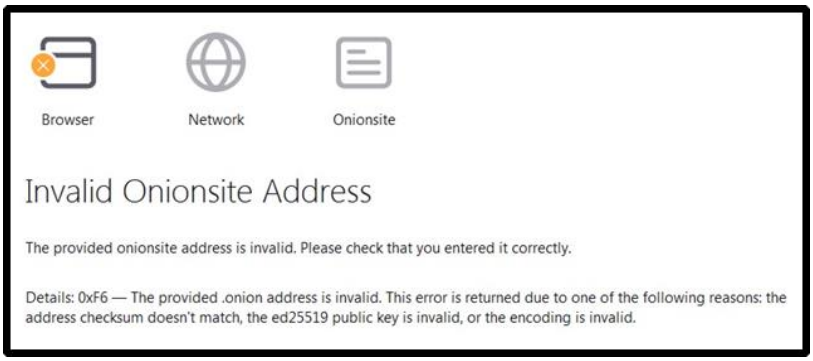
Redirection is frequent, as the servers go up and down and are run by private individuals and not companies with staff.

Many, many, forums are inactive with posting several years old.

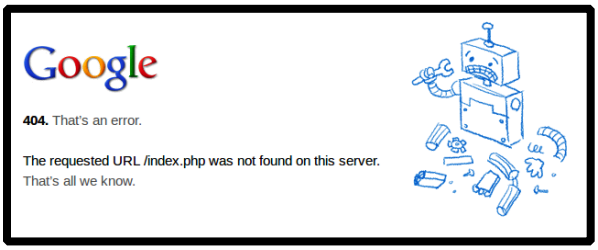

Site is down for maintainance.
Untill we are back check OnionDir for other Deep Web Tor hidden service .onion websites:
http://dirnxxdraygbifgc.onion/


Redirecting to hidden service.
You are being redirected to http://anonsteemnqvfma2.onion/.
If you are not redirected after a few seconds, please click on the link above!

On the Dark Web, you should get used to seeing a lot of this:


Browser
Network
Onionsite
Invalid Onionsite Address
The provided onionsite address is invalid. Please check that you entered it correctly.
Details: 0xF6 — The provided .onion address is invalid. This error is returned due to one of the following reasons: the address checksum doesn't match, the ed25519 public key is invalid, or the encoding is invalid.

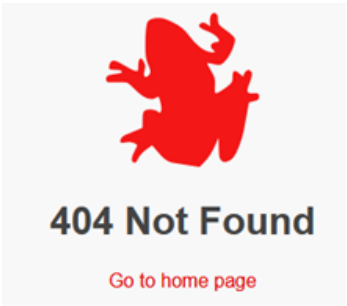
Rather than what you have been accustomed to on the Clear Web:

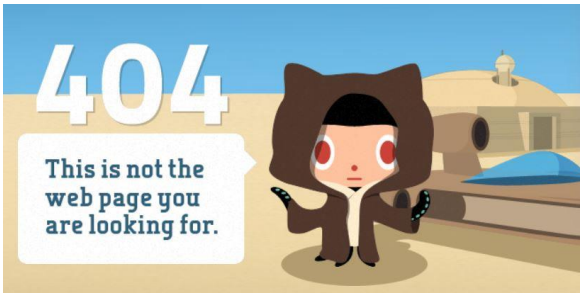


WARNING: use of Google is dangerous to your digital health

Or maybe even these:

404
Whoops! Page not found!
It may have moved or no longer exists, but the good news is we're working on it!
In the meantime, let's get you where you want to go:





50 of the most creative 404 pages on the web

https://www.canva.com/learn/404-page-design/

Typical DW Forum Rules (they have rules?)

As a free-speech platform, without the unjustified censoring provided by Clearnet sites such as Reddit, we will thrive to allow all content discussion and cater for as many different communities as we can. However, based on my own morals and issues of legality, it is essential that some ground rules are set in place to prevent unlawful content being shared on the platform.

Users must NOT, under any circumstances, post or privately discuss any of the following categories within the platform:

Child pornography
Pro-terrorism or terrorist propaganda
Harmful weapons/weapons of mass destruction
Poisons
Assassination services or media related to harm/murder

There are also community guidelines which all users much follow at all times:

1) No on-site trades/transactions of any sort.

2) No spam posts/comments/messages.

3) No vote brigading/manipulation. This includes requesting up votes from users.

4) No sharing of fear mongering content, with no factual basis or evidence. (AKA NO FUD)

5) No direct personal information of any individual. (AKA NO DOXXING)

6) No impersonating any known individual or staff member.

7) No spreading blatant misinformation in hopes of tricking those less intellectually fortunate (or high).

AND ABOVE ALL ELSE!

Anonymity is sacrosanct. Avoid discussion that may reveal too much about yourself or another user.

Other than these, use common sense, do not be an idiot, or abuse the free service in any way. These rules can be updated at any time.

A sample site:

/d/DarknetMarketsNoobs

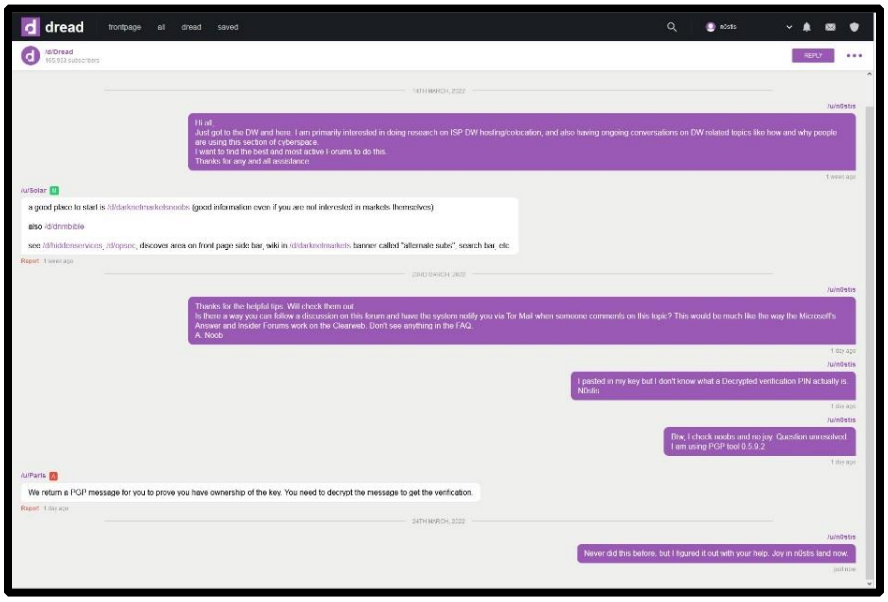
http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv-7jicoxknyazubrad.onion/d/DarknetMarketsNoobs

A place on dread for newbie's, newfers, NFG's, or here it is noobs i.e. everyone new to the Dark Web.

/d/DarknetMarketsNoobs

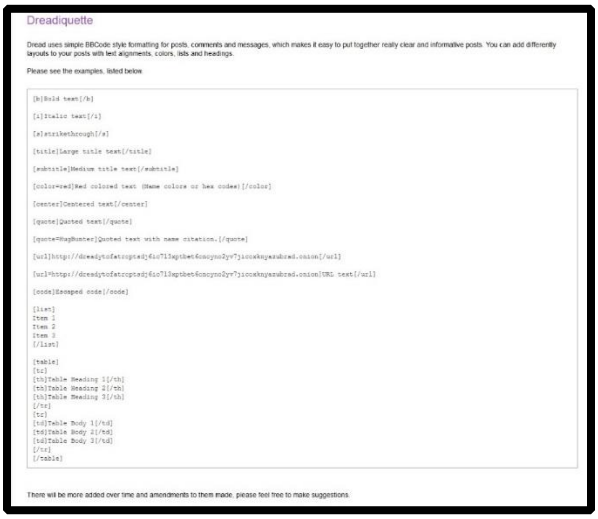
9,771 subscribers

This sub is for general and technical questions about using DNMs.


dread
frontpage
all
dread
saved
Hi all,
Just got to the DW and here. I am primarily interested in doing research on ISP DW hosting/colocation, and also having ongoing conversations on DW related topics like how and why people are using this section of cyberspace.
I want to find the best and most active f orums to do this.
Thanks for any and all assistance
a good place to start is
also
Thanks for the helpful tips. Will check them out.
Is there a way you can follow a discussion on this forum and have the system notify you via Tor Mail when someone comments on this topic? This would be much like the way the Microsoft's Answer and Insider Forums work on the Clearweb. Don't see anything in the FAQ.
A. Noob
I posted in my key but I don't know what a Decrypted verification PIN actually is
Nbdn
Btw, I check noobs and no joy. Question unresolved
I am using PGP tool 0.5.9.2
We return a PGP message for you to prove you have ownership of the key. You need to decrypt the message to get the verification.
Never did this before, but I figured it out with your help. Joy in nüsts land now.

dread Conversations

Dreadiquette


Dreadiquette

Dread uses simple BBCode style formatting for posts, comments and messages, which makes it easy to put together really clear and informative posts. You can add differently layouts to your posts with text alignments, colors, lists and headings.

Please see the examples, listed below

[b]Bold text[/b]

[i]Italic text[/i]

[s]strikethrough[/s]

[title]Large title text[/title]

[subtitle]Medium title text[/subtitle]

[color=red]Red colored text (Name colors or hex codes)[/color]

[center]Centered text[/center]

[quote]Quoted text[/quote]

[quote=RagHunter]Quoted text with name citation.[/quote]

[url]http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoknyazubrad.onion[/url]

[url=https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoknyazubrad.onion]URL text[/url]

[code]Escaped code[/code]

[list]
[*]Item 1
[*]Item 2
[*]Item 3
[/list]

[table]
[tr]
[th]Table Heading 1[/th]
[th]Table Heading 2[/th]
[th]Table Heading 3[/th]
[/tr]
[tr]
[td]Table Body 1[/td]
[td]Table Body 2[/td]
[td]Table Body 3[/td]
[/tr]
[/table]

There will be more added over time and amendments to them made, please feel free to make suggestions

DarknetHub

Your OneStop Hub for the Darknet

http://dnhuboxyxgbhmnozl5j4wntoon56x423-3iteusfmbqwsdwl26gnqgy6id.onion/

This site is either down or dead

About Us

Why and How

DarknetHub is an independent DarkNet research network and awareness programme administrated by anonymous research scholars studying Tor project (onion router) and websites accessible on the Tor browser. DarknetHub envisaged to created awareness about both legal and illegal content shared on the Darknet. We do not recommend users to visit any site mentioned in the articles or indexed in our portal(please read the disclaimer here). DarknetHub mainly researches privacy tools, cryptocurrency markets, independent shops, hidden communities and harm-reduction forums on the Darknet.

Although DarknetHub is also an anti-phishing resource and referencing directory for hidden sites, we do not take responsibility of the sites listed/indexed on our portal. Service administrators remove or add site links themselves. Fellow researchers/journalists are advised to learn using PGP keypairs and verifying PGP key signatures signed by the website owners. Accessing Darknet sites is mostly risky, sometimes simply visiting some sites itself is illegal. DarknetHub provides fellow researchers who are also curious about the Darknet a platform on finding the right research-worthy information and writing about communities on Tor.

All of these Dark Market and DW sites have some form of CAPTCHA to beat. Often times in multiple layers.

The Majestic Garden

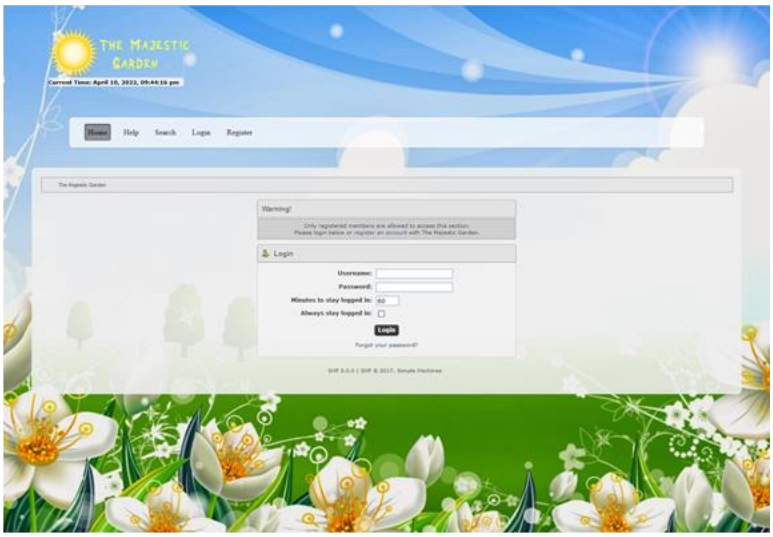
About The Majestic Garden Marketplace:

The Majestic Garden marketplace is dedicate to Psychedelic substances sale and uses direct P2P transactions.

http://talismanrestz7mr.onion

The Majestic Garden is not a usual DarkNet marketplace, rather is something like a psychedelics forum that also works as some of the DarkNet markets available all throughout the web. The DarkNet marketplace assists its users to utilize peer-to-peer (P2P) transactions in the process of buying and selling of the goods available in other DarkNet marketplaces. The Majestic Garden marketplace also aids the buyers by directing them to the stores or the accounts of the sellers in the entire established DarkNet marketplace.

http://garden4vzvrzyp4tks7llcwlynykllpq7qmm6jvuzf-3dgsg5jowzenad.onion/



Breaking Bad

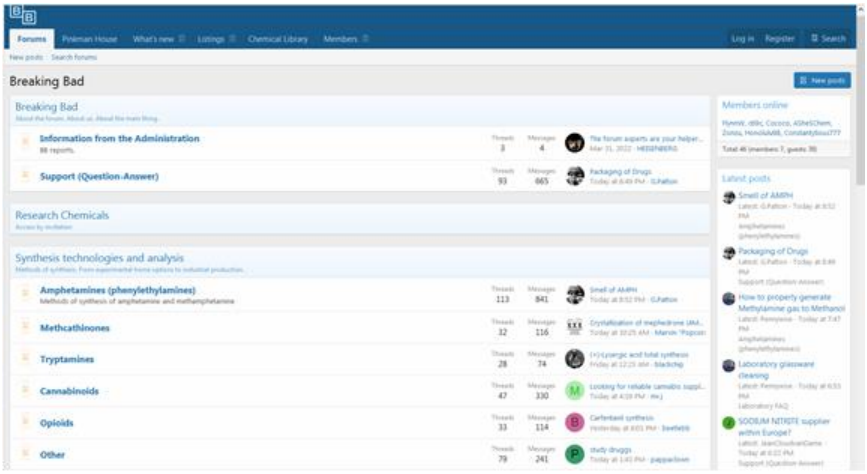
https://darkweblink.com/breaking-bad-forum/

bbzzzsvqcrqtki6umym6itiixfhni37ybtt7mkbjyxn2pgllzxf-2qgyd.onion

Breaking Bad is a Dark Web forum that welcomes professional participants of the DarkNet drug market. The forum gives the readers and the participants all information on organizing a laboratory of any size, be it a small kitchen at home or a great industrial zone. The forum is very useful for all those who own production and aims to help improve efficiency and safety with the relevant information.

All in all, the forum is very useful for all the aspirants and the users of the drug markets. The tutorials are worth mentioning as they are very descriptive.

Breaking Bad is a DarkNet forum on the Tor network that discusses various topics such as organic synthesis, chemical analysis, pharmacology, narcology, Internet technologies, data protection, marketing, trade-in specific equipment and substances, logistics and law. They also offer a ticket system where users can ask questions.



Incognito Market

Incognito is a newer marketplace on the DarkNet, but different from the more established ones when it comes to simplicity and loading speed. Since Incognito is a new market there might still not be this huge amount of listings and products as on the more established ones, but it is really worth checking it out and registering especially if you are interested in being a vendor and being early on upcoming and trending markets to get a head start.

How to access Incognito Market

If you already know how to use DarkNet, TOR and are familiar with the .ONION-network, then use the below URL or any mirror below to navigate to this Market.

Access Incognito at incognito.darkweb.wtf - this URL instantly redirects you to a working onion.

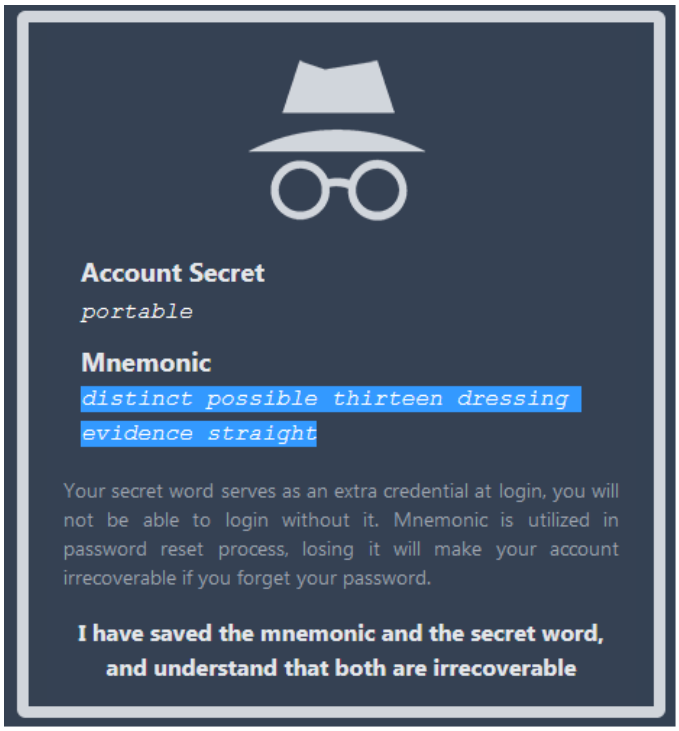
Link to Incognito Market incognito.darkweb.wtf

http://incognito2sjotqmbkys7wivkpq7d4a4tkpweoiqefk-7mpf7uvyfalad.onion/auth

ANONGUARD
incognito2sjotqm
bkys7wivkpq7d4a4
tkpweoiqefk7mpf7
uvyfa d(.)onion
Please complete the address
PROCEED
Address doesn't match?
Paste this in your url bar instead

User Name
I'm an employee
Secret Word
Password
Forgot your password?
Incognito
Captcha
Sign In
Not a member yet? Sign Up Now

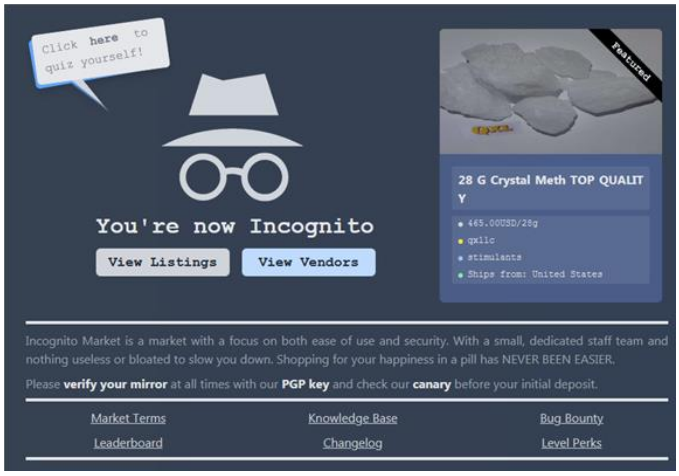
User Name
Password
Repeat Password
Incognito
Captcha
Sign Up


Account Secret
portable
Mnemonic
distinct possible thirteen dressing evidence straight
Your secret word serves as an extra credential at login, you will not be able to login without it. Mnemonic is utilized in password reset process, losing it will make your account irrecoverable if you forget your password.
I have saved the mnemonic and the secret word, and understand that both are irrecoverable

If you get it wrong

Personal Punk
Dear user, welcome to the Incognito family. This personal punk is randomly generated and will represent you in transactions and user interactions!
Yay! Continue to Market

If you get it right.


Click here to quiz yourself!
You're now Incognito
View Listings
View Vendors
Featured
28 G Crystal Meth TOP QUALIT Y
465.00USD/28g
qxllc
stimulants
Ships from: United States
Incognito Market is a market with a focus on both ease of use and security. With a small, dedicated staff team and nothing useless or bloated to slow you down. Shopping for your happiness in a pill has NEVER BEEN EASIER.
Please verify your mirror at all times with our PGP key and check our canary before your initial deposit.
Market Terms
Knowledge Base
Bug Bounty
Leaderboard
Changelog
Level Perks

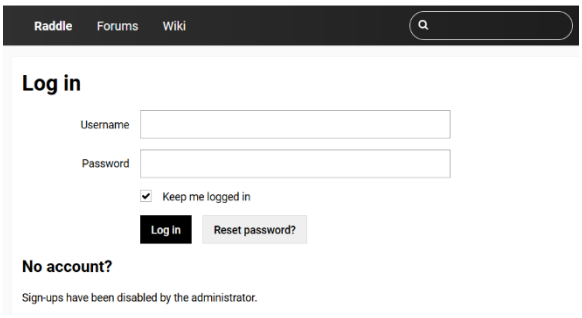
As I previously mentioned, this book has no interest in documenting the illegal transactions conducted in the previously mentioned forums.

To quote Robbie Robertson, *This is where I get off, this ain't where I belong, this is where I move on.*

I do however have an interest in conversing and understanding why people visit the legal or dual use onion sites like Raddle, dread, The Hub and Envoy.

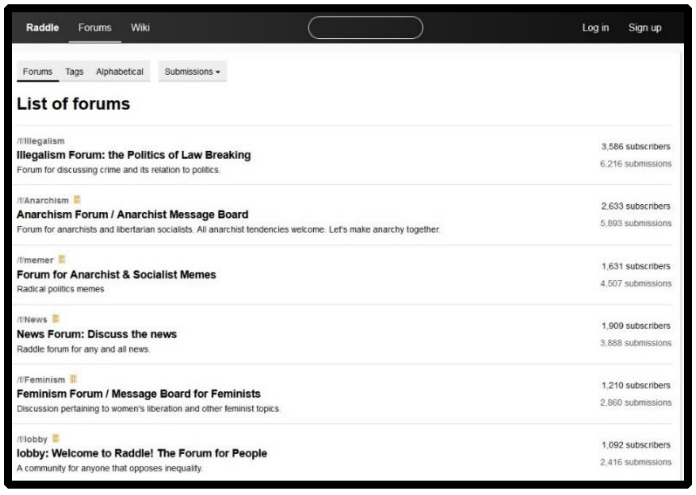
Raddle

Massive number of forums from Ability to Zoom
https://raddle.me/ (ME= Montenegro)



Signups disabled? No soup for me, guess I will try the onion site.

c32zjeghcp5tj3kb72pltz56piei66drc63vkhn5yixiyk-4cmerrjtid.onion



After some poking around and messaging it turns out that this onion site is just a mirror site of raddle.me.

So it is not the Dark Web, just a seedier part of the Clear Web (DarkNet) run from a foreign country.

/f/AskRaddle

Where am I and why am I here?

Submitted by n0stis on April 25, 2022 at 5:22 PM in AskRaddle (edited on April 25, 2022 at 5:24 PM)

7 comments

Viewing a single comment thread. View all comments

veuzi wrote on April 25, 2022 at 9:12 PM

This is an anarchist alt-reddit on the clearnet (raddle.me) with a darknet option. There's not that much more to it.

n0stis OP wrote on April 26, 2022 at 6:14 PM

Thanks for the info. To be clear, you are saying that the onion site http://c32zjeghcp5tj3kb72pltz56piei66drc63vkhn5yixiyk4cmerrjtid.onion/ is just a mirror of raddle.me?

veuzi wrote on April 26, 2022 at 9:43 PM

Correct.

So not really the Dark Web here, and deeper down the rabbit hole we will now go.

The Hub

Members: 80511 • Posts: 308479 • Topics: 16667

The Hub includes a discussion forum on Tor hidden services on the Dark Web focused on Dark Web market reviews, cryptocurrency and security.

https://darkweblink.com/the-hub/

The Hub forum links

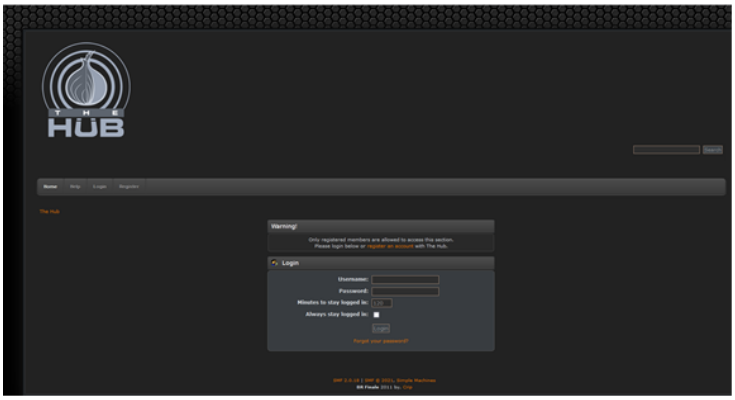
thehubmcwyzwijjoqvdtpmu36npcueypjbgnvbqz-4jliwjmmnpfkzkqd.onion

thehubojcm5xduv2yvoc4tmn5jf4e2hssnlxu66uuknus-3jutim7g7ad.onion

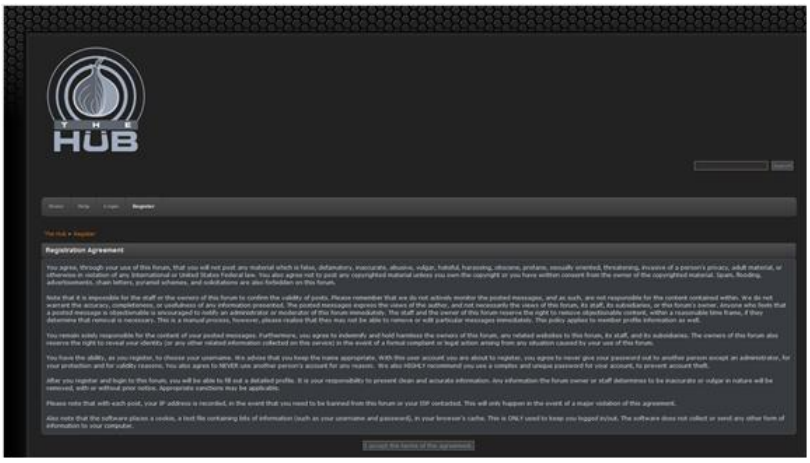
thehubrysnv5i7mlaitavqjosqgcnbaimk2c4hesgamno-7boyvxxokid.onion

thehubwav7canwaq7trm6zl3tqvkf-2kwbkgwvwonfssvgvtyrdy4u3yd.onion

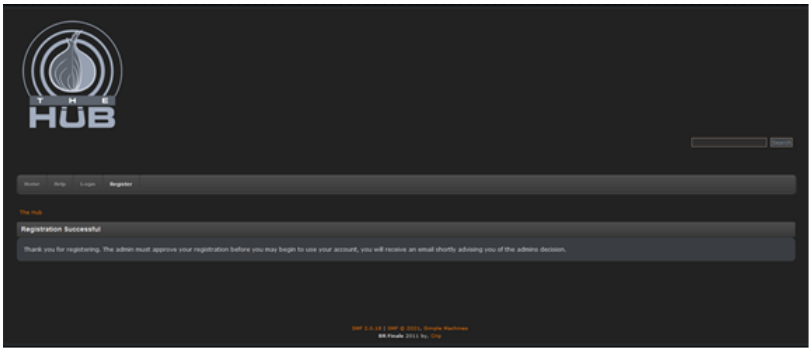
thehubwevkaz2jqh3xiyalbfxljj6drmilqyz2j4jbeltmo-2n3wbiqqd.onion



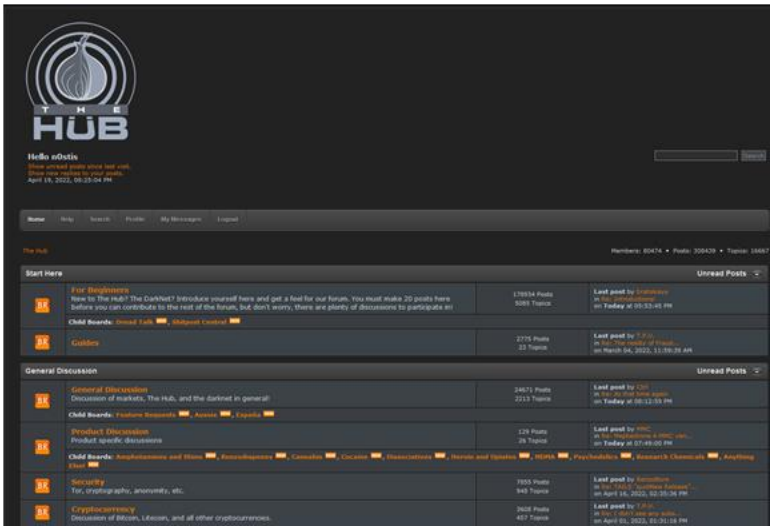
Username, secret word, password and beat CAPTCHA. No sweat!



Agree to the terms

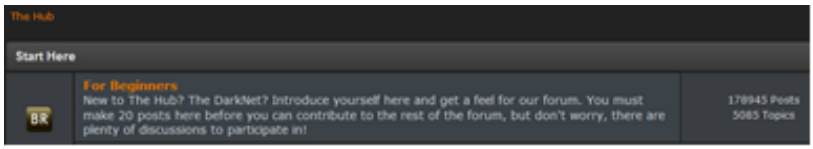

THE HUB
Registration Successful
Thank you for registering. The admin must approve your registration before you may begin to use your account, you will receive an email shortly advising you of the admins decision.

So we wait to be approved by the administrator.



Approved and ready to go. But wait…

You must Post 20 times at the Beginners Forum (sit at the kids table) before you are allowed to Post in the main forums (be seated at the adults table).


The Hub
Start Here
For Beginners
New to The Hub? The DarkNet? Introduce yourself here and get a feel for our forum. You must make 20 posts here before you can contribute to the rest of the forum, but don't worry, there are plenty of discussions to participate in!
178943 Posts
5085 Topics

Then you get to select an optional avatar, my hero and role model George Jetson

The Hub Rules & Regulations

This post will outline how you should conduct yourself during your time here. Please read it thoroughly before using The Hub, and remember to check back regularly in case of changes. Failure to comply could lead to account deletion or suspension.

1. No Trading

You may not facilitate trades using The Hub, either via public message boards or our PM system. There are no exceptions to this rule, and users found doing so will be either warned, suspended or deleted depending on the circumstances. If spotted, please report any violation of this rule to a staff member for investigation.

2. When Promoting Products You Sell:

a) You may only link to your official marketplace vendor profile when posting. Do not make posts discussing your products or services without including a link to your marketplace profile. That is what the marketplaces are for.

b) You must be verified as a vendor and have the "Vendor" tag

Quote from: Alfred on January 09, 2014, 04:17:32 PM

New as of 16/10/2019

Read the following, carefully

Click the orange quote to be taken to the vendor verification thread

c) You must not attempt to promote trade via any other means such as Email - even if the market you vend on is currently out of action.

3. Prohibited Items

The promotional discussion of certain items, and discussion that endorses certain behaviors, is not permitted. As a general rule, prohibited items and topics should be considered those that are designed to harm others, or harm others by their design. This includes (but is not limited to) items and topics on the following list:

- Child Pornography

- Fraud

- ID theft

- Hacking

- Weapons

- Explosives

It is natural that these items and topics may surface in natural, non-promotional, objective discussion, and we believe that in most circumstances there is no harm in this.

4. No 'Doxing'

We are all members of a relatively anonymous community. Please respect one another's anonymity and never post details, suspected or known, regarding a community member's 'Real Life' identity.

This also applies to self-harm and attaching a valid, deliverable, Clearnet or other unsafe e-mail address to an anonymous identity - effectively deanonymyzing it.

5. No Spam

Spam comes in many forms, such as: Advertisements; links to malicious content; content with zero value. The Hub is not a place for posting this kind of content, and spammers will have their accounts and posts deleted.

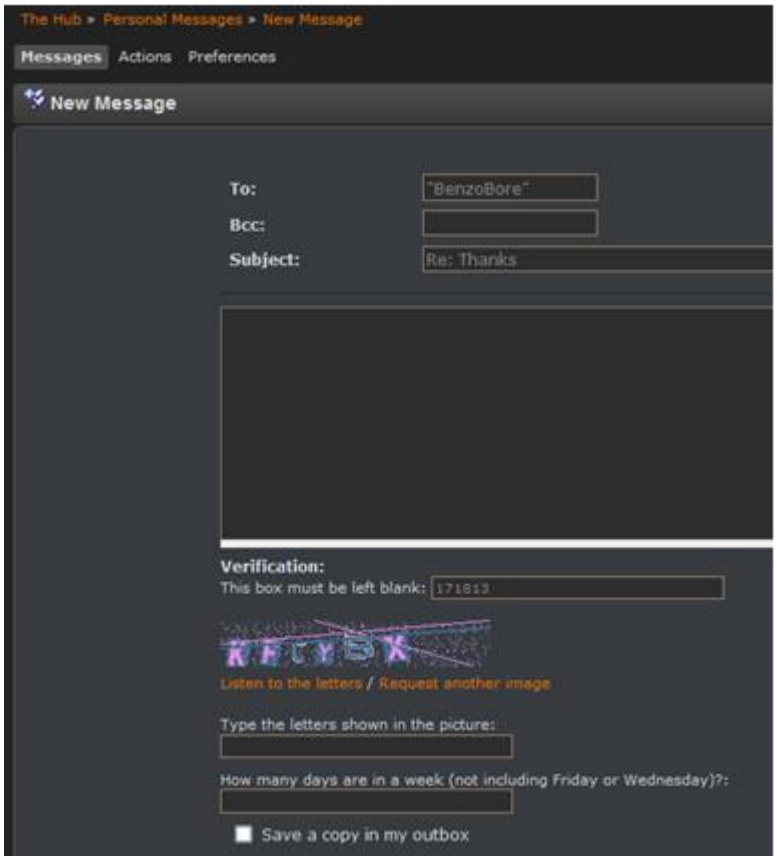
6. No Trolling

According to Wikipedia: "In Internet slang, a troll is a person who sows discord on the Internet by starting arguments or upsetting people, by posting inflammatory, extraneous, or off-topic messages in an online community (such as a forum, chat room, or blog), either accidentally or with the deliberate intent of provoking readers into an emotional response or of otherwise disrupting normal on-topic discussion"

Trolls are not looked upon kindly; their accounts may be restricted or banned, and their posts may be removed or moved to an appropriate sub-forum.

You must spam to 20 in the proper thread to post in main threads of the forum.

Please enjoy your time here at The Hub, and as with anything incredible, use responsibly!



I found that when responding to posts and PM's, that the CAPTCHA was most difficult to read. I usually needed to click on the Listen to the letters link (in a new tab) and then click on the direct link which will open your media player and read the letters to you.

The pronunciations are purposely misleading but between hearing and seeing the letters you can usually figure it out in one or two tries. This patience trying pain the butt is probably why there are not more members.

And now we can see some of the unedited level of discourse on The Hub. Certainly makes you wonder about the next generation.

STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« on: April 25, 2021, 03:52:33 AM »

Scrolling through some 200+ new account registrations and having to delete account after fucking account because stupid fucking imbeciles are still using gmail, yahoo, outlook emails with what looks like REAL IRL NAMES!!! Get a fucking grip its 2021 not 2011.

Thank you.

benihana:

secmail accounts are not allowed. (their website was compromised and we do not trust them any more).com accounts are not allowed (just.write.anything.in.the.field@not.really.important)

« Last Edit: January 12, 2022, 09:58:26 AM by benihana »

"You are entitled to your own opinion, but not your own facts"

- Zaphod

These modern scam felchers bring nothing to the table, waste of bandwidth and physical space.-mst

"I genuinely want more, as long as someone keeps that text restrained within quotes. I don't want the superflous overflow of spectacular words amounting to an unworldly word mountain"- benihana

Allegiance

- *Head Punch Monkey*
- *Global Moderator*
- *Legendary Contributor*
- *Posts: 3107*
- *Community Rating: +226/-77*
- *Drunk on power and high on Mod Crack*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #1 on: April 25, 2021, 04:33:28 AM »

Sigh... It's like people are de-evolving instead of evolving.

Guys we've been doing server upgrades, patches and improvements that we won't go into detail, but regardless of that, guess what? LE IS AMONGST US! SAY HELLO!

Yes, ladies and gents, this forum is being actively scraped and surveilled by LE among others. What a fucking shocker!!! If only there was a way we could obfuscate our identities and our personal data... oh, wait, but there is! IT'S CALLED FUCKING PGP!! IT'S ALSO CALLED SECMAIL, ELUDE, ANY FUCKING DARK NET EMAIL PROVIDER THAT IS IN NO WAY ASSOCIATED TO YOUR REAL IDENTITY!!!!!!!!

In fact you don't even need a goddamned email to get on here, just put any old shit in the field and be done with it! It's that fucking easy!

But Allie, you say, how can we be here knowing the FBI/CIA/NSA/INTERPOL/MOSSAD/WHATEVER are watching us? Very easy:

1) Fuck Windows and everything else, learn to use TAILS

2) PGP evething

3) DON'T IN ANY WAY SHAPE OR FORM link your real identity to your DN activities!!

I could go on and on but honestly I have better things to do with my time if by now you don't get it.

If you can't be here the right way, it's best you not be here at all. Allie

"Allie often shares the mod crack with me " -T.P.V

"You don't have to be a weirdo to mod here but it helps " -Lucidity

"my wife is a non binary black transsexual amphibious all terrain attack trained doormat i beg your pardon very much

still smells fishy, you better wash behind your ears and other places too"- Benihana

"Anyone who doesn't like pineapple on pizza is a cunt" - Lucidity

T.P.V.

- *Moderator*
- *Legendary Contributor*
- *Posts: 2269*
- *Community Rating: +129/-77*
- *If you're new welcome. If you're lost try Guides.*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #2 on: April 25, 2021, 09:58:19 AM »

lol LU is not happy.

I shall msg him my new gmail address to cheer him up. .

Please read the HUB rules before posting. Encrypt PM's people.

lucidity

- *Global Moderator*
- *Hero Contributor*
- *Posts: 1679*
- *Community Rating: +180/-46*
- *Sensei of the Taco Shits*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #3 on: April 25, 2021, 07:41:54 PM »

Quote from: thepeoplesvoices on April 25, 2021, 09:58:19 AM

lol LU is not happy.

I shall msg him my new gmail address to cheer him up. .

I am only trying to save people from their own idiotic foolishness.

"You are entitled to your own opinion, but not your own facts"

- Zaphod

These modern scam felchers bring nothing to the table, waste of bandwidth and physical space.

-mst

"I genuinely want more, as long as someone keeps that text restrained within quotes. I don't want the superflous overflow of spectacular words amounting to an unworldly word mountain"

- benihana

wanderer

- *Jr. Contributor*
- *Posts: 82*
- *Community Rating: +6/-15*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #4 on: April 25, 2021, 10:24:51 PM »

I think the Registration Agreement needs an update. For the sake of everyone.

lucidity

- *Global Moderator*
- *Hero Contributor*
- *Posts: 1679*
- *Community Rating: +180/-46*
- *Sensei of the Taco Shits*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #5 on: April 26, 2021, 01:58:58 AM »

Quote from: wanderer on April 25, 2021, 10:24:51 PM

I think the Registration Agreement needs an update. For the sake of everyone.

you think we need to include a statement that says please do not use your real name or real email when signing up for a darknet forum where the most common topic of discussion is drugs? or should we include a section for home address, SSN and LinkedIn profile?

"You are entitled to your own opinion, but not your own facts"

- Zaphod

These modern scam felchers bring nothing to the table, waste of bandwidth and physical space.

-mst

"I genuinely want more, as long as someone keeps that text restrained within quotes. I don't want the superflous overflow of spectacular words amounting to an unworldly word mountain"

- benihana

T.P.V.

- *Moderator*
- *Legendary Contributor*
- *Posts: 2269*
- *Community Rating: +129/-77*
- *If you're new welcome. If you're lost try Guides.*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #6 on: April 26, 2021, 05:40:42 AM »

Quote from: lucidity on April 25, 2021, 07:41:54 PM

Quote from: thepeoplesvoices on April 25, 2021, 09:58:19 AM

lol LU is not happy.

I shall msg him my new gmail address to cheer him up. .

I am only trying to save people from their own idiotic foolishness.

Oh I get it LU I just don't think we can save em. If they are that stupid you know they are not encrypting addresses for orders.

Please read the HUB rules before posting. Encrypt PM's people.

wanderer

- *Jr. Contributor*
- *Posts: 82*
- *Community Rating: +6/-15*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #7 on: April 26, 2021, 02:03:42 PM »

Quote from: lucidity on April 26, 2021, 01:58:58 AM

Quote from: wanderer on April 25, 2021, 10:24:51 PM

I think the Registration Agreement needs an update. For the sake of everyone.

you think we need to include a statement that says please do not use your real name or real email when signing up for a darknet forum where the most common topic of discussion is drugs? or should we include a section for home address, SSN and LinkedIn profile?

If it makes your job easier, then yes. Might save a few people from self-doxing as well.

Report to moderator Logged

Allegiance

- *Head Punch Monkey*
- *Global Moderator*
- *Legendary Contributor*
- *Posts: 3107*
- *Community Rating: +226/-77*
- *Drunk on power and high on Mod Crack*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #8 on: April 27, 2021, 08:09:15 AM »

Quote from: wanderer on April 26, 2021, 02:03:42 PM

Quote from: lucidity on April 26, 2021, 01:58:58 AM

Quote from: wanderer on April 25, 2021, 10:24:51 PM

I think the Registration Agreement needs an update. For the sake of everyone.

you think we need to include a statement that says please do not use your real name or real email when signing up for a darknet forum where the most common topic of discussion is drugs? or should we include a section for home address, SSN and LinkedIn profile?

If it makes your job easier, then yes. Might save a few people from self-doxing as well.

Dude, on paper you have a valid point and it will be done eventually. In reality, people don't give a shit and DON'T READ. If you don't believe me, go ask anybody over at TMG. Fuck, don't even ask or go, just look at their section here and then tell me again how the magical registration agreement will solve everybody's problem.

Allie

"Allie often shares the mod crack with me " -T.P.V

"You don't have to be a weirdo to mod here but it helps " -Lucidity

"my wife is a non binary black transsexual amphibious all terrain attack trained doormat i beg your pardon very much

still smells fishy, you better wash behind your ears and other places too"- Benihana

"Anyone who doesn't like pineapple on pizza is a cunt" - Lucidity

T.P.V.

- *Moderator*
- *Legendary Contributor*
- *Posts: 2269*
- *Community Rating: +129/-77*
- *If you're new welcome. If you're lost try Guides.*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #9 on: April 27, 2021, 05:01:09 PM »

Quote from: Allegiance on April 27, 2021, 08:09:15 AM

Quote from: wanderer on April 26, 2021, 02:03:42 PM

Quote from: lucidity on April 26, 2021, 01:58:58 AM

Quote from: wanderer on April 25, 2021, 10:24:51 PM

I think the Registration Agreement needs an update. For the sake of everyone.

you think we need to include a statement that says please do not use your real name or real email when signing up for a darknet forum where the most common topic of discussion is drugs?

or should we include a section for home address, SSN and LinkedIn profile?

If it makes your job easier, then yes. Might save a few people from self-doxing as well.

Dude, on paper you have a valid point and it will be done eventually. In reality, people don't give a shit and DON'T READ. If you don't believe me, go ask anybody over at TMG. Fuck, don't even ask or go, just look at their section here and then tell me again how the magical registration agreement will solve everybody's problem.

Allie

It is Allie for the win. +1

Please read the HUB rules before posting. Encrypt PM's people.

Unnoen117

- *Brand Spankin' New*
- *Posts: 1*

- *Community Rating: +0/-0*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #10 on: April 28, 2021, 11:13:41 AM »

lol

Newman

- *New Contributor*
- *Posts: 22*
- *Community Rating: +5/-2*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #11 on: May 01, 2021, 05:23:45 PM »

Quote from: lucidity on April 26, 2021, 01:58:58 AM

Quote from: wanderer on April 25, 2021, 10:24:51 PM

I think the Registration Agreement needs an update. For the sake of everyone.

you think we need to include a statement that says please do not use your real name or real email when signing up for a darknet forum where the most common topic of discussion is drugs? or should we include a section for home address, SSN and LinkedIn profile?

Wait.....so yo don't want my Linkedin? My experience speaks for itself.....

auspride

- *New Contributor*
- *Posts: 23*
- *Community Rating: +3/-0*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #12 on: August 18, 2021, 01:58:05 AM »

Lol welcome to The Hub!

Report to moderator Logged

maybelater

- *Brand Spankin' New*
- *Posts: 6*
- *Community Rating: +0/-0*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #13 on: September 10, 2021, 12:07:33 AM »

Thats true, but im fcking trying to create an email for a week and all services arent working for some reasons. i ve tried tutanota, it wont let me in my fresh account saying that my password is incorrect (although i am just copying it from my password manager), elude mail, but i connected to the onion web page only once and then it stopped answering, same for proton mail. i ve tried torbox, but when im triyng to login it says that theres some IMAP problems and doesnt work too. so for now im left with only guerilla temporary adresses.

maybe theres some new darknet email services that are working in 2021? help me plz

lucidity

- *Global Moderator*
- *Hero Contributor*
- *Posts: 1679*
- *Community Rating: +180/-46*
- *Sensei of the Taco Shits*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #14 on: September 10, 2021, 03:33:47 AM »

Quote from: maybelater on September 10, 2021, 12:07:33 AM

Thats true, but im fcking trying to create an email for a week and all services arent working for some reasons. i ve tried tutanota, it wont let me in my fresh account saying that my password is incorrect (although i am just copying it from my password manager), elude mail, but i connected to the onion web page only once and then it stopped answering, same for proton mail. i ve tried torbox, but when im triyng to login it says that theres some IMAP problems and doesnt work too. so for now im left with only guerilla temporary adresses.

maybe theres some new darknet email services that are working in 2021? help me plz

You are missing the point competely

When registering an account here do not use a real email just make something up

Example

fakenotreal@email.gofuckyourself.ru

"You are entitled to your own opinion, but not your own facts"

- Zaphod

These modern scam felchers bring nothing to the table, waste of bandwidth and physical space.

-mst

"I genuinely want more, as long as someone keeps that text restrained within quotes. I don't want the superflous overflow of spectacular words amounting to an unworldly word mountain"

- benihana

IDinnaeGetItMan

- *Jr. Contributor*
- *Posts: 51*
- *Community Rating: +7/-15*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #15 on: September 10, 2021, 07:56:30 PM »

have seen some new vendors lately using real clearnet emails on pgp

oh well, more low hangers makes life safer for the rest to some degree

maybelater

- *Brand Spankin' New*

- *Posts: 6*
- *Community Rating: +0/-0*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #16 on: September 11, 2021, 12:12:51 AM »

Quote from: lucidity on September 10, 2021, 03:33:47 AM

Quote from: maybelater on September 10, 2021, 12:07:33 AM

Thats true, but im fcking trying to create an email for a week and all services arent working for some reasons. i ve tried tutanota, it wont let me in my fresh account saying that my password is incorrect (although i am just copying it from my password manager), elude mail, but i connected to the onion web page only once and then it stopped answering, same for proton mail. i ve tried torbox, but when im triyng to login it says that theres some IMAP problems and doesnt work too. so for now im left with only guerilla temporary adresses.

maybe theres some new darknet email services that are working in 2021? help me plz

You are missing the point competely

When registering an account here do not use a real email just make something up

Example

fakenotreal@email.gofuckyourself.ru

but why is there a necessary email to use on this hub then? would it be safer to just make it unnecessary so that only the ones who wants to get some feedback would put their emails there?

anyways I still want to have a working email account. so my question is still relevant.

Report to moderator Logged

benihana

- *Hero Contributor*
- *Posts: 674*
- *Community Rating: +429/-231*
- *reformed troll*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #17 on: September 13, 2021, 06:17:59 AM »

Quote from: maybelater on September 11, 2021, 12:12:51 AM

Quote from: lucidity on September 10, 2021, 03:33:47 AM

Quote from: maybelater on September 10, 2021, 12:07:33 AM

Thats true, but im fcking trying to create an email for a week and all services arent working for some reasons. i ve tried tutanota, it wont let me in my fresh account saying that my password is incorrect (although i am just copying it from my password manager), elude mail, but i connected to the onion web page only once and then it stopped answering, same for proton mail. i ve tried torbox, but when im triyng to login it says that theres some IMAP

problems and doesnt work too. so for now im left with only guerilla temporary adresses.

maybe theres some new darknet email services that are working in 2021? help me plz

You are missing the point competely

When registering an account here do not use a real email just make something up

Example

fakenotreal@email.gofuckyourself.ru

but why is there a necessary email to use on this hub then? would it be safer to just make it unnecessary so that only the ones who wants to get some feedback would put their emails there?

anyways I still want to have a working email account. so my question is still relevant.

The email function is disabled in the forum code. It's simply not functional

It can't be used because it could be abused.

Remember, this is a safe place. We put mandatory mittens on your lil' hands and then sit you around the fire so you can hear scary stories

Report to moderator Logged

Quote from: | Click here to read rules and regulations | on February 20, 2014, 08:28:47 PM

Mandatory reading prior to communication attempts. Most unencrypted PMs are trashed.

Olympus

- *New Contributor*
- *Posts: 37*
- *Community Rating: +5/-1*
- *While we rise others will fall!*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #18 on: September 13, 2021, 02:17:44 PM »

I can't believe my eyes! People still do that?!

And then they wonder how they got caught?

sn2sfdqay6cxztroslaxa36covrhoowe6a5xug6wlm6ek7nmeiujgvad.onion

2b4byl0ns

- *Brand Spankin' New*
- *Posts: 2*
- *Community Rating: +0/-0*

Re: STOP USING YOUR REAL EMAILS YOU FUCKING IDIOTS

« Reply #19 on: September 15, 2021, 03:56:13 AM »

This is really sad. "Oh boy I found a forum on the darknet!!! I be hakzor now!!" Sad people have to learn the hard way. When I started, hotmail was

all we really had to use. I made 20 something accounts and rotated them. Burned them after about 6 months then made new ones. I think I came across a darknet 101 type video on youtube that talked about things to keep in mind for newbies. Maybe someone can find it and link to it so people have to watch it before making an account.

FatherTed,

Thanks for your reasonable and correct response. The

"Save a copy to my outbox" check mark introduces the idea of an outbox and there actually isn't one. There is just Sent items

As a long time Outlook email user, I am accustomed to both.

The Hub »Personal Messages » Inbox

Gives the impression that there is an Outbox. This is what I was looking for.

However, regardless of messages in the Inbox you still need to hover (an evil Windows term I guess) the mouse over the Messages button to see the Sent Items dropdown.

I am not sure why these people need to diminish others so intently, when their own shortcomings are so apparent.

-----BEGIN PGP MESSAGE-----

-----END PGP MESSAGE-----

My most recent login attempt resulted in:

502 Timeout

It seems this endgame front doesn't have a stable connection to the backend right now.

To fix it you can try to reload the page. If that doesn't work, and you end back here, get a new circuit.

If getting a new circuit doesn't work. Try to get a brand new Tor identity.

If getting a new Tor identity doesn't work come back later.

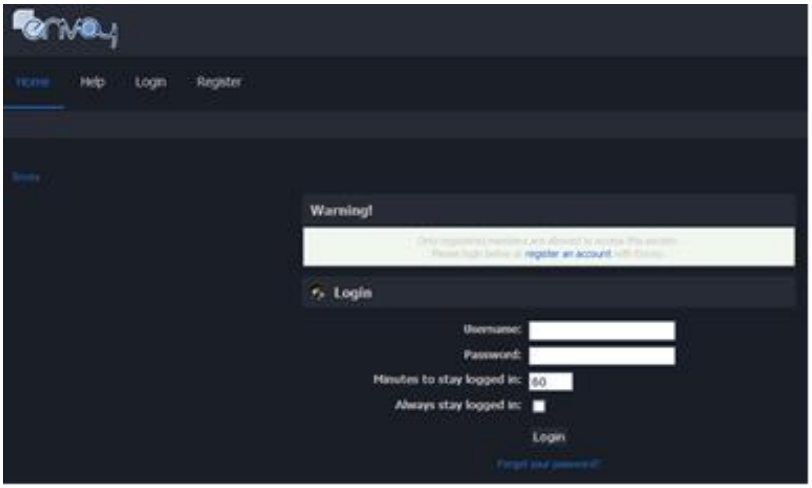
Ok, so I am not a guest I was trying to log in.

Envoy

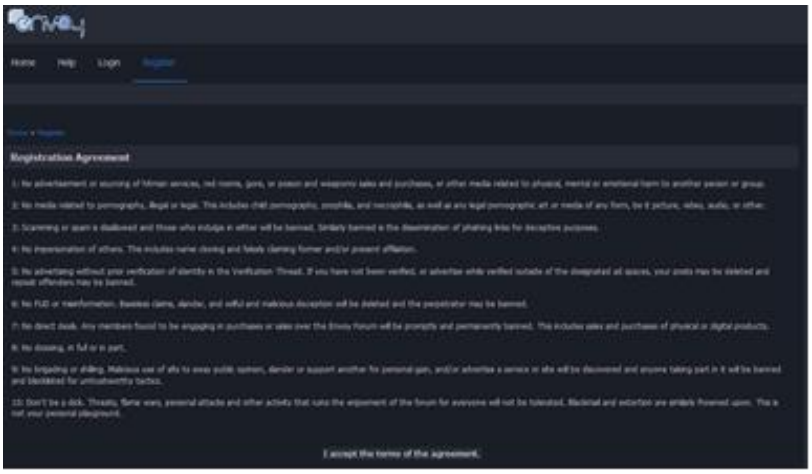
Envoy Forums 4094 members

General, Drugs, Dark Net Markets, Cyber Insecurity, The One Stop Onion Shop, Health and Joy, and The Bouncy Castle

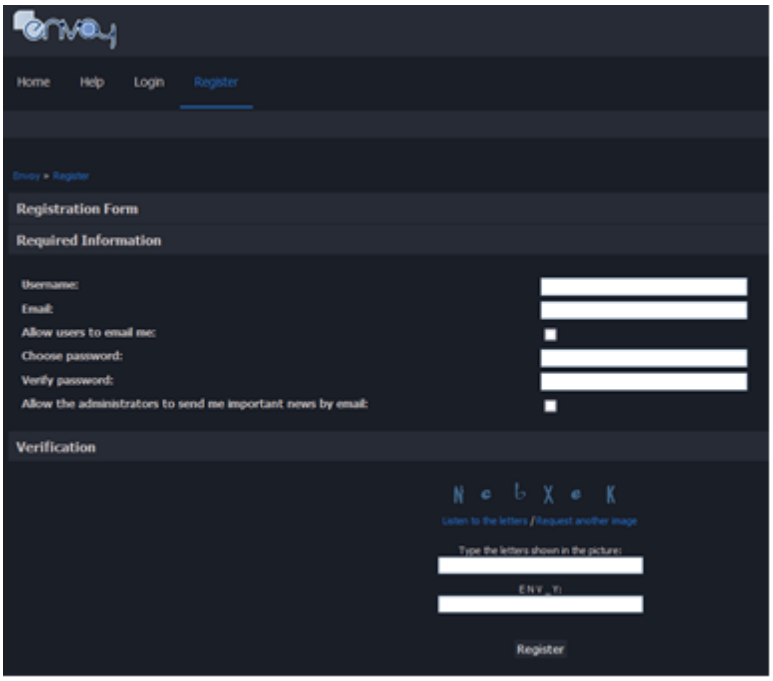
http://envoy2vxtsbz63bik33yb6vka2ed4x5leeisfg2isd2gz-2eg4skwmbyd.onion/



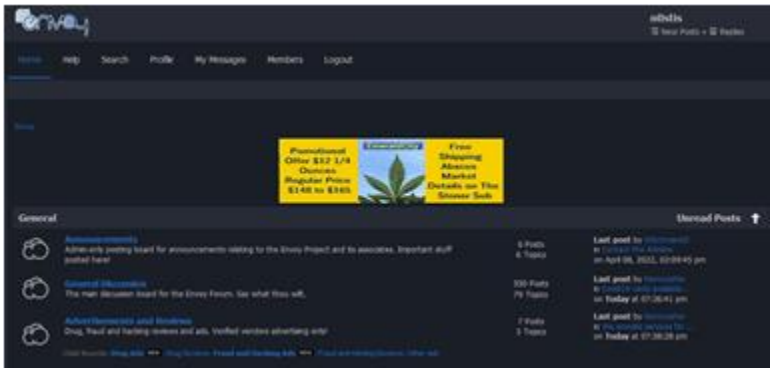
Splash page



Agreement



Login with CAPTCHA



Home page

Forum messaging

Private messaging

Sample message ad in Envoy.

Topic: Real and authentic Documents (Read 27 times)

Envoy

emmaneulla

- *Newbie*
- *Posts: 1*
- *Penis Size +0/-0*
- *New Ambassador*

Real and authentic Documents

- *Quote*

Telegram….@Darknetdocsforsale))Where to Obtain Valid-Fake Documents Online

We are a Team of IT Experts specialized in the production of Real and authentic Documents such as

\Passport, Driving License, Covid19 Vaccine Cards, CSCS Cards, Ship license, Boating License,

Diploma Certificates, PhD's, IELTS Certificate, Bachelor degrees, NCLEX Certificate, MBA, ID Cards,

SS Cards, Associate Certificate, University Certificates, Green Cards, Death Certificate, Master

Degree, PMP Certificate, Working Permits, Visa's etc.

Contact us on WhatsApp for more

Your job side on request for covid-19 card? we offer registered covid19 vaccine card at affordable prices without getting vaccinated,

we produce registered cdc vaccination cards at affordable prices, you want to travel or at your job site on requestour aim is to help

those who shy aay from the cdc vaccine to obtain the card so as to show proof of being vaccinated

A blank Covid-19 vaccination record card; a filled-in version has become many people's prized possession. contact us for more details.

Why Did the "Torigon" Dark Web Forum Fail so Hard?

Torigon is an example of how things work in the Dark Web and the amount of work required to keep a successful platform up. "Torigon" was a new English-speaking cybercrime forum that entered the Dark Web scene with impetus in October 2019. The fact that it no longer exists serves as an exemplary case of how the field works.

https://www.technadu.com/torigon-dark-web-forum-fail-hard/105576/

dread

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv-7jicoxknyazubrad.onion/auth/login

What is Dread?

A review of dread with history and purpose

https://dnstats.net/site/dread-2/

Short version:

dread is like the Reddit for the Dark Web, without the censoring and privacy problems of its Clear Web cousin.

Longer version:

Dread is an onion based free speech platform and forum, where you can post, comment and share among tons of different communities.

It was developed with both privacy and usability in mind, choosing to stick to a common user interface to match the likes of Reddit, but without the added security issues that are involved with the use of JavaScript.

It was developed by /u/HugBunter in early 2018 and launched on February 16th.

Following a month of down time from the 23rd of April, the platform was redeveloped to be a lot more stable, with the backbone and UI completely re-imagined to allow for more flexibility, based on the mistakes that were made in the first iteration.

> *"Initially, I planned to base the communities solely around my interest in DarkNetMarkets and the security surrounding them, but since then it has grown to become much more than that, housing a variety of different communities and providing a safe place for users to interact without the fear of censorship beyond the specific rules in place. We provide a hub for harm reduction to many aspects of Deep Web purchases, including, but not limited to, security reports and also safe drug use information." /u/HugBunter*

This message perhaps tells more of the story.

Hello beautiful peeps.

by /u/sn0w • in /d/OpSec

The site is designed like butter.. big shoutouts to the dev team and the people behind this place... It has almost 200k people active on here daily and it has been online for a couple of years now..

/u/donkeysquadreborn

dat rite reddit stole paris and hugs site design thats why they aint make it open source no more,

In this case, I believe that this choice of language is a paranoid reaction to being identified (de-anonymized) based on writing style and word usage.

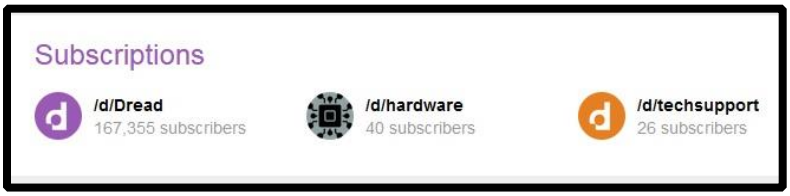
/d/Dread has 167,000 subscribers

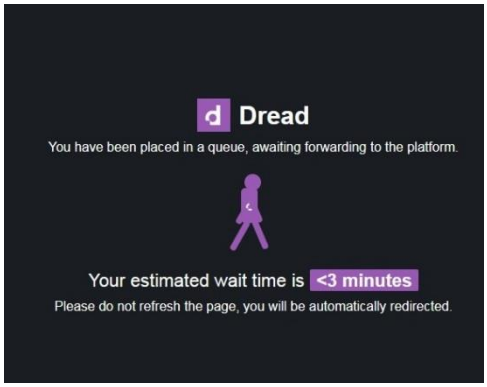
(The official community for Dread announcements, discussion, and feedback. **(others much less)**

/d/OpSec 15,000 (Operational Security, how to be safe on the DW)

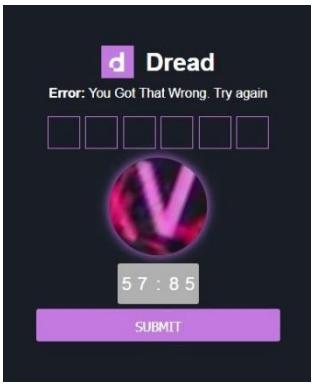
/d/DarkNetMarkets 34,000 (buying and selling guns, drugs, etc.)

/d/Carding 10,000 (buying and selling stolen credit cards or numbers)



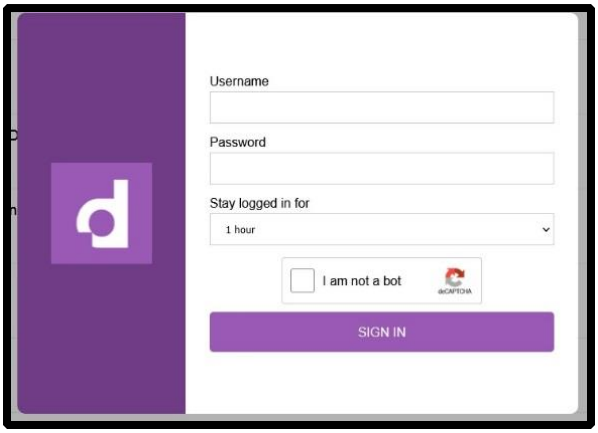

Dread
You have been placed in a queue, awaiting forwarding to the platform.
Your estimated wait time is <3 minutes
Please do not refresh the page, you will be automatically redirected.

Dread onion page waiting room



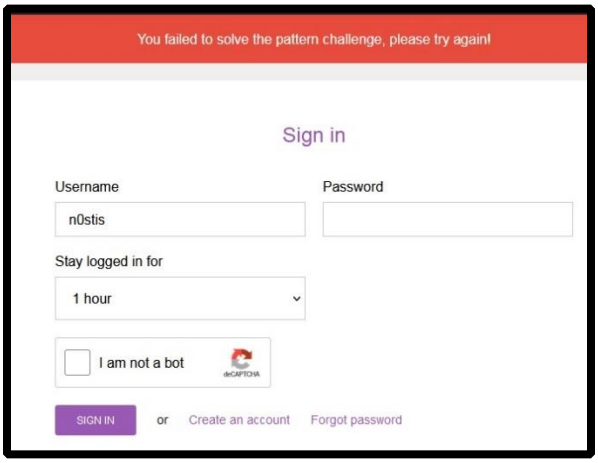
Initial dread onion page CAPTCHA

The initial dread login page (a fill in the blanks image CAPTCHA.



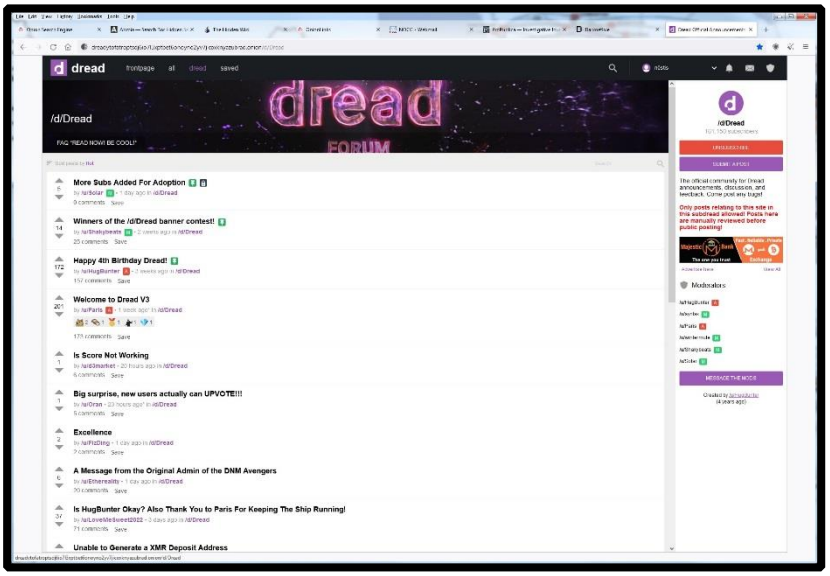
The most active forum n0stis had seen spelunking around the Dark Web.

The dread login page (a rotating image CAPTCHA of three images which must be put to the correct rotation orientation) is very easy on the brain and once a photo has been rotated correctly it just seems right (besides the occasional photo that lacks any visual ques for correct rotation).



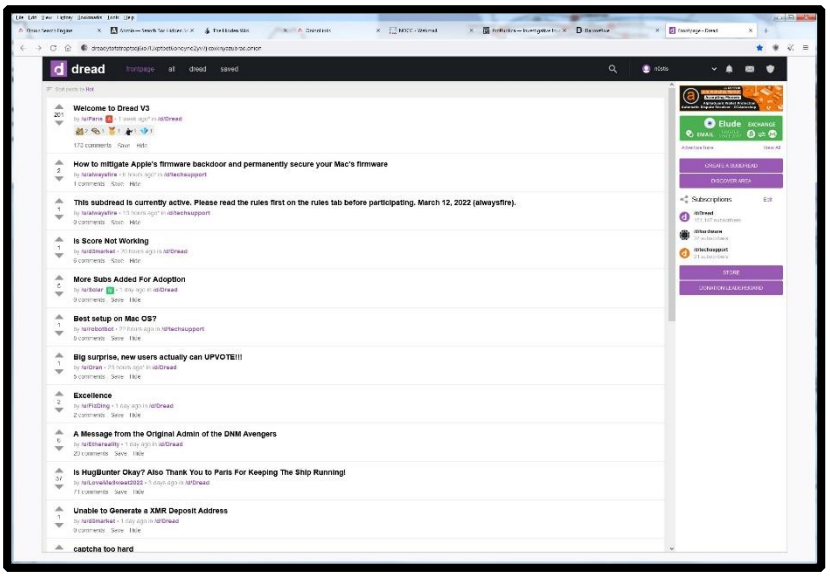
If you fail the CAPTCHA Turing test , you get this red message.

dread Forum site


dread
/d/Dread
FORUM
More Subs Added For Adoption
Winners of the /d/Dread banner contest!
Happy 4th Birthday Dread!
Welcome to Dread V3
Is Score Not Working
Big surprise, new users actually can UPVOTE!!!
Excellence
A Message from the Original Admin of the DNM Avengers
Is HugBunter Okay? Also Thank You to Paris For Keeping The Ship Running!
Unable to Generate a XMR Deposit Address

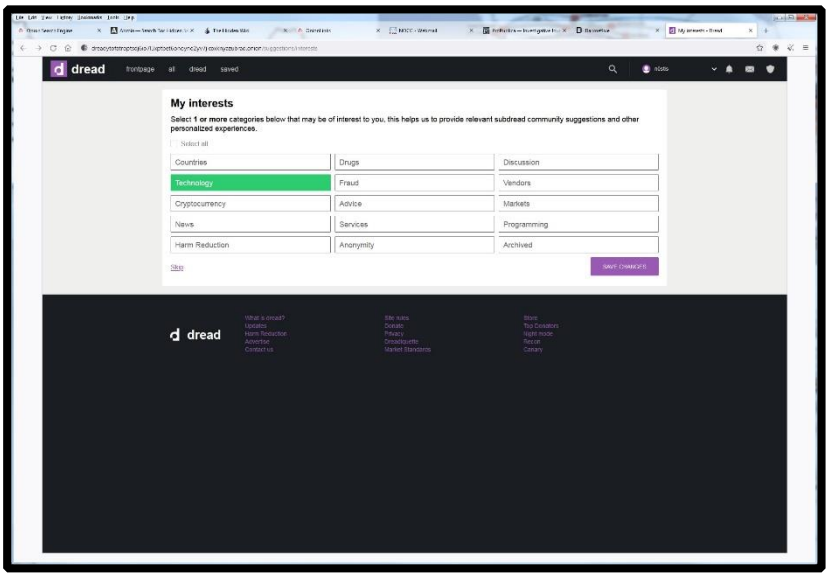
dread Forum site

dread Frontpage


dread
frontpage
all
dread
saved
Welcome to Dread V3
How to mitigate Apple's firmware backdoor and permanently secure your Mac's firmware
This subdread is currently active. Please read the rules first on the rules tab before participating. March 12, 2022 (alwaysfire).
Is Score Not Working
More Subs Added For Adoption
Best setup on Mac OS?
Big surprise, new users actually can UPVOTE!!!
Excellence
A Message from the Original Admin of the DNM Avengers
Is HugBunter Okay? Also Thank You to Paris For Keeping The Ship Running!
Unable to Generate a XMR Deposit Address
captcha too hard
Subscriptions

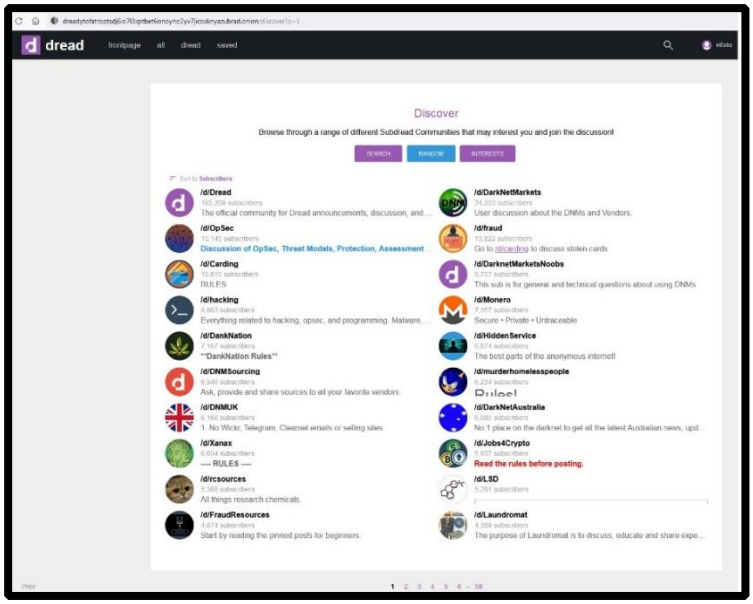
dread frontpage

My Interests



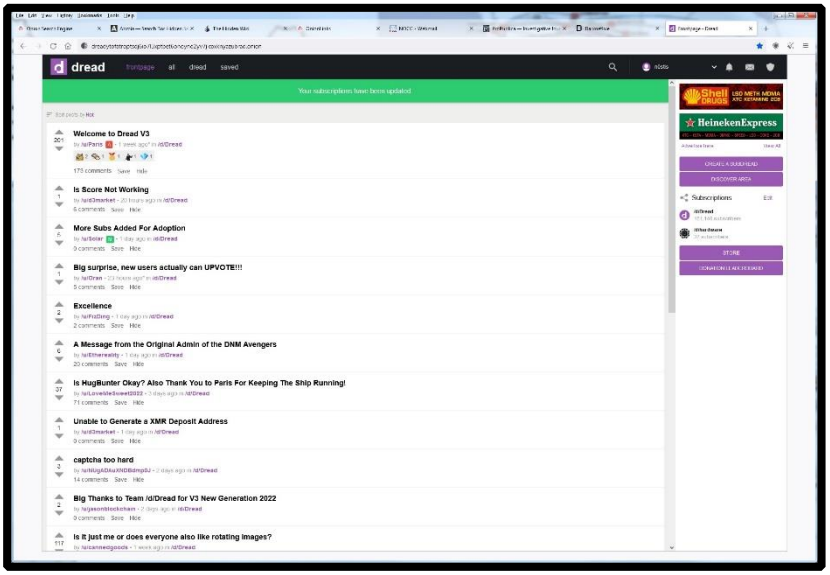
Pick your interest areas

dread Discover

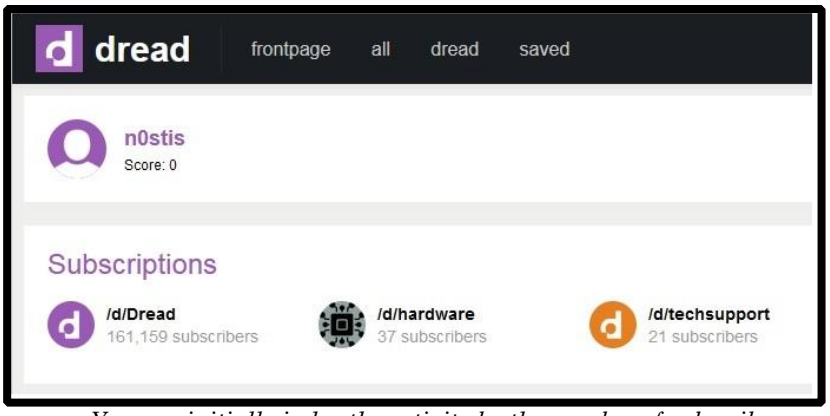


Select forum topic of interest to subscribe to

The Forum


dread
frontpage
all
dread
saved
Your subscriptions have been updated
Welcome to Dread V3
Is Score Not Working
More Subs Added For Adoption
Big surprise, new users actually can UPVOTE!!!
Excellence
A Message from the Original Admin of the DNM Avengers
Is HugBunter Okay? Also Thank You to Paris For Keeping The Ship Running!
Unable to Generate a XMR Deposit Address
captcha too hard
Big Thanks to Team /d/Dread for V3 New Generation 2022
Is it just me or does everyone also like rotating images?
HeinekenExpress

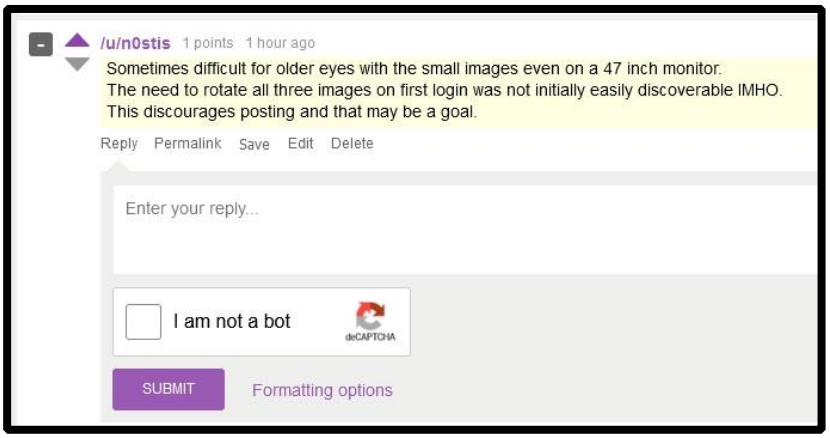
An interestingly complex forum interface



You can initially judge the activity by the number of subscribers.

Messages are sent using your username with the sub as /u/n0stis (example)

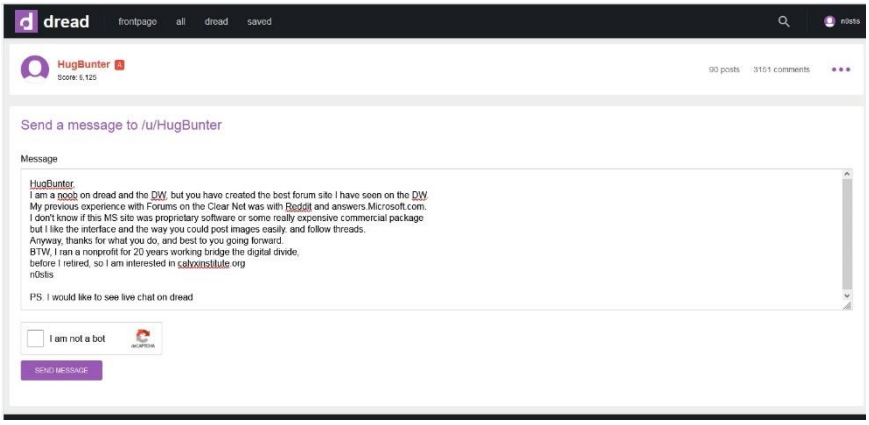
The rotating image CAPTCHA is required for all postings to keep the bots and spam away unless you sign up for the $50 per month premium account service.


/u/n0stis 1 points 1 hour ago
Sometimes difficult for older eyes with the small images even on a 47 inch monitor.
The need to rotate all three images on first login was not initially easily discoverable IMHO.
This discourages posting and that may be a goal.
Reply Permalink Save Edit Delete
Enter your reply...
I am not a bot
reCAPTCHA
SUBMIT
Formatting options

Some users have the star trophy which lets them bypass the captcha, but that is something not given out very often. In the past, it has been given it to contest winners, or some people that have been with Dread for a very long time and contributed a lot.

Messages

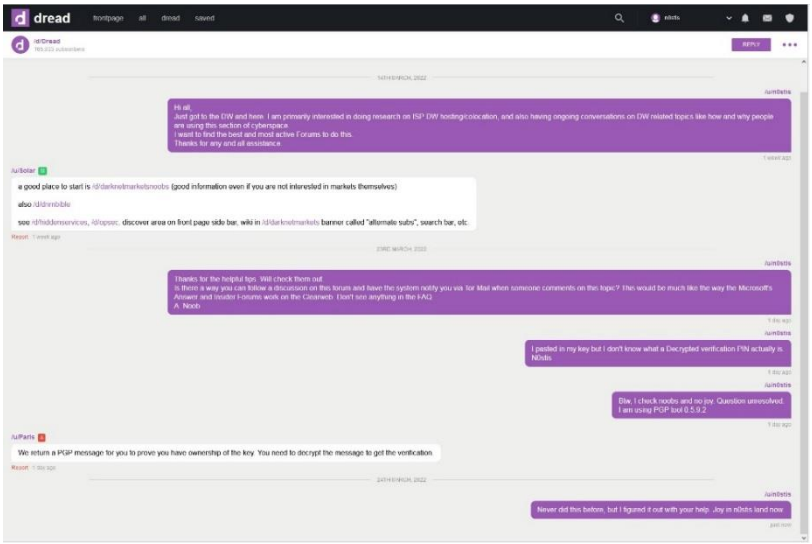
Messages lead to conversations


dread
frontpage
all
dread
saved
HugBunter
Score: 6,125
90 posts
3151 comments
Send a message to /u/HugBunter
Message
HugBunter,
I am a noob on dread and the DW, but you have created the best forum site I have seen on the DW.
My previous experience with Forums on the Clear Net was with Reddit and answers.Microsoft.com.
I don't know if this MS site was proprietary software or some really expensive commercial package
but I like the interface and the way you could post images easily, and follow threads.
Anyway, thanks for what you do, and best to you going forward.
BTW, I ran a nonprofit for 20 years working bridge the digital divide,
before I retired, so I am interested in calyxinstitute.org
n0stis
PS. I would like to see live chat on dread
I am not a bot
SEND MESSAGE

Creating a message

Conversations

You can message other forum members in clear text using their profile names.


dread
frontpage
all
dread
saved
REPLY
Hi all,
Just got to the DW and here. I am primarily interested in doing research on ISP/ DW hosting/colocation, and also having ongoing conversations on DW related topics like how and why people are using this section of cyberspace.
I want to find the best and most active Forums to do this.
Thanks for any and all assistance
a good place to start is
also
see
Thanks for the helpful tips. Will check them out.
Is there a way you can follow a discussion on this forum and have the system notify you via for Mail when someone comments on that topic? (He would be much like the way the Microsoft's Answer and Insider Forums work on the Clearweb. I don't see anything in the FAQ.
A. Noob
I posted in my key but I don't know what a Decrypted verification PIN actually is.
N0stis
Btw, I check noobs and no joy. Question unresolved.
I am using PGP tool 0.5.9.2
We return a PGP message for you to prove you have ownership of the key. You need to decrypt the message to get the verification.
Never did this before, but I figured it out with your help. Joy in n0stis land now

For example:

matter replies:

"Thank you. Let me know if you need any help at all or if you want information on certain topics. I have hosted stuff on VPS for many years, like web sites (Clearnet & .onion), VPN servers, proxy servers, VNC etc. Take care."

n0stis replied:

matter,

So, I created a pdf file which is a first draft of a document on basic web hosting that I thought might be of use in a sub like noobs or a web hosting one, which I don't believe yet exists here.

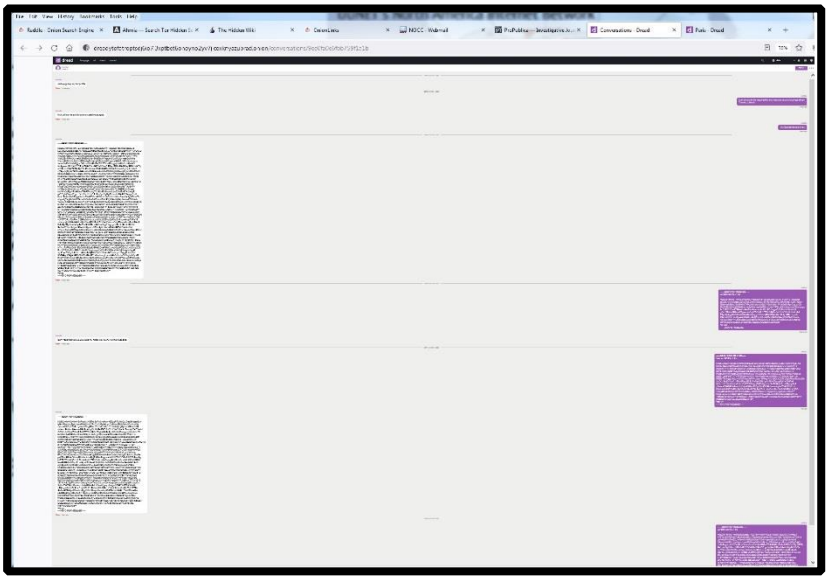
Do you think that this might be a good idea, and would you be willing to review it?

Do I encrypt it and send Clearnet or just send it to your Tor email (which I don't have)?

Don't know what is the proper protocol and am looking to contribute to this forum, not just take.

n0stis

Or you can communicate with encrypted conversations.



You can also toggle to a different reader mode. Change reader view to simple text (F9).

Conversations – dread (example)

Hi all,

Just got to the DW and here. I am primarily interested in doing research on ISP DW hosting/colocation, and also having ongoing conversations on DW related topics like how and why people are using this section of cyberspace.

I want to find the best and most active Forums to do this.

Thanks for any and all assistance.

Thanks for the helpful tips. Will check them out.

Is there a way you can follow a discussion on this forum and have the system notify you via Tor Mail when someone comments on this topic? This would be much like the way the Microsoft's Answer and Insider Forums work on the Clear Web. Don't see anything in the FAQ.

A. Noob

I pasted in my key but I don't know what a decrypted verification PIN actually is.

n0stis

Btw, I check noobs and no joy. Question unresolved.

I am using PGP tool 0.5.9.2

A mod replied:

We return a PGP message for you to prove you have ownership of the key. You need to decrypt the message to get the verification.

Never did this before, but I figured it out with your help. Joy in n0stis land now.

Rather than collocating a server, have any recommendations on reputable hosting services?

1 week ago in /d/Dread

Sometimes difficult for older eyes with the small images even on a 47 inch monitor.

The need to rotate all three images on first login was not initially easily discoverable IMHO.

This discourages posting and that may be a goal.

Am new to the DW and new here. Have 25 years professional hardware experience. Would be HTH. Am interested in DW related topics mostly.

dreadytofatroptsdj6io7l3xptbet6onoyno2yv-7jicoxknyazubrad.onion

Thanks for creating this amazing platform : /d/Dread

by /u/Claude in /d/Dread

I'm really grateful for what you are doing. People have don't' realize how difficult it is to set up an infrastructure like this. First of all, you have to be a security expert. You have to design the system very carefully to mitigate potential DDoS attacks.

For the frontend, you can't even use JavaScript! And yet you managed to do it. I don't know who wrote the code (I think /u/Paris and /u/HugBunter), but mad respect for creating this.

I think this website is awesome. I discover so many interesting things. It's like how I imagine the Internet has been in the early 2000's.

Anyways, thanks for everything!

n0stis – Dread

by /u/n0stis in /d/hardware

1988 Exec PC Milwaukee 2400bps

1990 Spry in Seattle Win 3.1 Usenet, gopher, Archie 4800bps

1992 CompuServe @9600bps, 14,4, 28.8, 56k.

1995 ISDN and DSL, Win95 and IE

The speed and costs were generally horrendous. But the fun was there before everything was assimilated into the corporate (Microsoft, Google, Apple, Facebook) Borg.

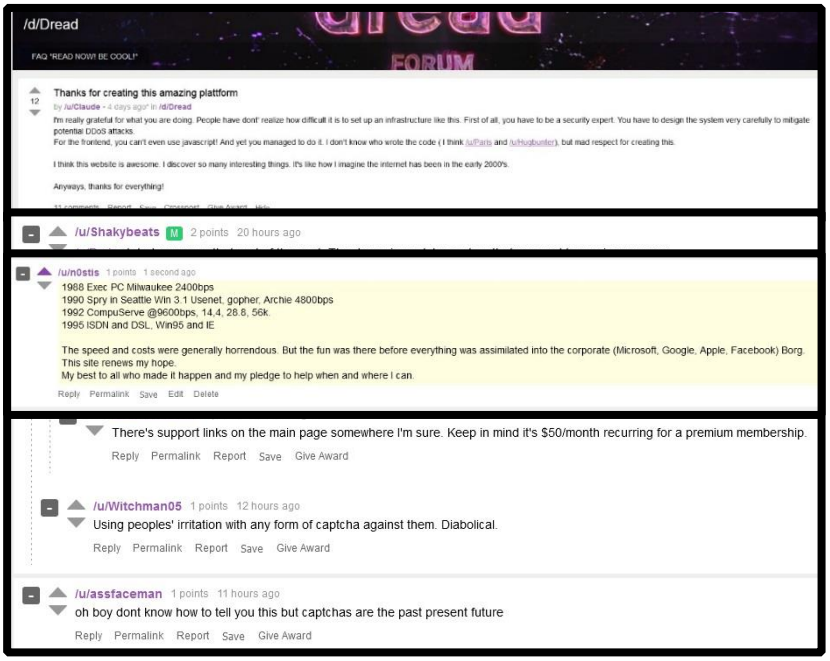
This site renews my hope.

My best to all who made it happen and my pledge to help when and where I can.

Discussions on dread subs

Discussions on the dread site and its use of CAPTCHA in the /d/dread sub (clear text)

dreadytofatroptsdj6io7l3xptbet6onoyno2yv-7jicoxknyazubrad.onion??


/d/Dread
FAQ "READ NOW!! BE COOL!"
FORUM
Thanks for creating this amazing plattform
I'm really grateful for what you are doing. People have dont' realize how difficult it is to set up an infrastructure like this. First of all, you have to be a security expert. You have to design the system very carefully to mitigate potential DDoS attacks.
For the frontend, you can't even use javascript! And yet you managed to do it. I don't know who wrote the code (I think and), but mad respect for creating this.
I think this website is awesome. I discover so many interesting things. It's like how I imagine the internet has been in the early 2000's.
Anyways, thanks for everything!
/u/Shakybeats M 2 points 20 hours ago
/u/n0stis 1 points 1 second ago
1988 Exec PC Milwaukee 2400bps
1990 Spry in Seattle Win 3.1 Usenet, gopher, Archie 4800bps
1992 CompuServe @9600bps, 14,4, 28.8, 56k.
1995 ISDN and DSL, Win95 and IE
The speed and costs were generally horrendous. But the fun was there before everything was assimilated into the corporate (Microsoft, Google, Apple, Facebook) Borg.
This site renews my hope.
My best to all who made it happen and my pledge to help when and where I can.
Reply Permalink Save Edit Delete
There's support links on the main page somewhere I'm sure. Keep in mind it's $50/month recurring for a premium membership.
Reply Permalink Report Save Give Award
/u/Witchman05 1 points 12 hours ago
Using peoples' irritation with any form of captcha against them. Diabolical.
Reply Permalink Report Save Give Award
/u/assfaceman 1 points 11 hours ago
oh boy dont know how to tell you this but captchas are the past present future
Reply Permalink Report Save Give Award

And this is how the Dark Web Dark Market's go down for good.

Well... That's All Folks!

by /u/WilliamGibson ✶S TΛF F ✶ • 2 days ago in /d/Versus

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA512

Dear Community,

There is no doubt that there has been a lot of concern and uncertainty regarding Versus in the last few days. Most of you that have come to know us have rightfully assumed that our silence has been spent working behind the scenes to evaluate the reality of the proposed vulnerability. After an in-depth assessment, we did identify a vulnerability which allowed read-only access to a 6+ month old copy of the database as well as a potential ip leak of a single server we used for less than 30 days. We take any and every vulnerability extremely seriously but we do think that its important to contend a number of the claims that were made about us. Specifically of importance: there was no server pwn and users/vendors have nothing to worry about as long as standard and basic opsec practices have been utilized (for example, PGP encryption)

In many ways, we are glad to see the community coming together to improve everyone's security, this was our dream from the beginning with Versus, though we will say that there was a clear agenda behind the way this was originally handled, but we leave you to draw your own conclusions

Once we identified the vulnerability, we were posed with a fork in the road, to rebuild and come back stronger (as we had done before) or to gracefully retire. After much consideration, we have decided on the latter. We built Versus from scratch and ran for 3 years. We built a community and even became the #1 DNM when we never intended for that to be the goal. At a certain point, there is no further way up to go, only down, and in this business it is best to not make decisions out of pride. While we are not ending on the note that we would have liked, we hope that the truth about the actual scope of the vulnerability, combined with the impact we have had on the community, leaves users remembering Versus fondly for years to come. Versus Market has officially retired and we thank you for your support and being part of something that hopefully defined the future of DNM's.

For all our vendor:

We will soon publish a link where you guys can get your transactions without the locktime. No need to wait 90 days.

It was a good run and I would like to thank you all.

All the best,

William Gibson

-----BEGIN PGP SIGNATURE-----

iQKTBAEBCgB9FiEEFAl5ki+ljOnGotMlXFDURnuuQqEFAmKKRLJf
FIAAAAAALgAo

aXNzdWVyLWZwckBub3RhdGlvbnMub3BlbnBncC5maWZ0aGhvcnNl
bWFuLm5ldDE0

MDk3OTkyMkZBNThDRTlDNkEyRDMyNTVDNTBENDQ2N0JBRTQ
yQTEACgkQXFDURnuu

QqHryQ/+IAUfX7anIWAESD5AIPz/gBt9ufFovPHWl13SCDghpgt9v0
Zu6zv03WSK

1e/RlVUTXfAfMdyvlXCMy6ItdtEsQi4dBHzy/exgr9Obrg0NLu4ie1poyp
7c3+Vk

h3Ok6PX2FcCSKMNTZUYa0z7ycHK+NOop+IfG/MErPVRx0eVMvjC
QRw3+QMgVm75P

NqnCh1bdesOReMAbnMrdqTLWTfgIxAXJ4KMhxbawBx1SWg+34wBc
HbTjGh/SIlHI

vTBN6ROt3bxc6M+8JPxAMb9+Ai1h1rcqgYy+T3wW3bkP97eEtbkOI4j
KwsUhyiLQ

Zoq9PNkzRRIiyxzttdBB49tWGUewGKTgnWlmQc4LEcMGK13jAu0uJ2
r+wsq24Kl3

YuQjzkN8bZCLqFyy+Zdu1uJszER1RGSFTk6QtMBztlNHGX7XpDQX
bz+4OXhwCzj

ag58VyosXNI51LPEuzNlNWszE6r+HuS0Jcjh6ImsMYL6NlhmZ+uz2z
WVXO1xL90O

eTx4Zb3kCWHSppUZJivnEd6I3tvgE1pfkP9y2R9RmcWif9JPsnNwCsc
3pzStrPAE

c26wWvrKeEU5Gr+5PYMY3YDciTSUnER/k8/s9bCUm7v+NkIyJAOb
2fNOmL8gSl8e

pQ0kYSAedfNSiQptiK6lEK+0d5oDy99MTxWGbHNY2Y+akisl/v4=
=QV1O

-----END PGP SIGNATURE-----

Some more discussion in dread:

Serious Question.

by /u/maxwellhill • 20 hours ago in /d/CafeDread

Who is the smartest people in Dread for you.

8 comments

/u/capobianco

Hugbunter and Paris, their knowledge is the greatest.

/u/maxwellhill

Yes, also its very hard to be an Dread or any kind of tor forum admin. You must be have good Opsec.

/u/Nobcheese

Impossible to say, but I've got huge respect for the dread admins. To do what they do for so long without getting caught takes a lot of intelligence and drive.

In terms of a broader community, probably the folks over in /d/Carding. Carding isn't as easy as they make it seem. Shit's hard.

/u/maxwellhill

Thank you for your answer.

/u/Playable

What if the og admins are long dead and now these new ones are just fbi agents running their setup as a project to rid of our money when the time comes?

I mean you said it yourself that they haven't been caught for the longest, it could be a thing, just saying

/u/Nobcheese

Haha imagine. If they've done that then they are the smartest people on Dread. They haven't though.

/u/dickinmyass

Definitely not DeSnake and StarScream. But besides them, we are all smart here.

Paranoia on dread

Feds collecting context data on dread. To identify us IRL

by /u/TweakCity • 1 hour ago in /d/CafeDread*

I understand and can see why vendors communicate in one form of context and one form only.

How much more longer do you think we have? Till they can ID us fast enough just by dialoguee on the DN.

Mods delete this post in /d/cafedread when you can

/u/foshizzledizzle

/u/shakybeats

I should of posted this in /d/opsec

19 comments

/u/dickinmyass knuckle sandwich in your face

Honestly, what I'm personally more worried of are the nude pictures I've posted all over reddit and 4chan. They definitely have me captured from head to toe.

As for your question, I think this is still far to unlikely for now to arrest someone just based on his text.

/u/TweakCity

I'm not referring to being arrested. You're right. They have to collect other pieces of evidence before they can even do something like that.

But, technology is going to become very advanced one day. I would not be surprised if they can ID us by first and last name from our linguistic from a few contexts of text.

/u/dickinmyass knuckle sandwich in your face

Yes. I've edited my reply. And yes.. as much as paranoid it might sound, you are not wrong.

/u/AutoModerator M Fuck You

"No matter how paranoid you are, what they're actually doing is worse than you can possibly imagine."

This comment was posted automatically by a bot. All AutoModerator settings are configured by individual communities. Contact this community's Moderators to have your post approved if you believe this was in error.

/u/TweakCity

It's not paranoia at all. This is real.

/u/AutoModerator M Fuck You

For example, a user sees a duck on the river and thinks the police have placed a camera in the duck to watch him.

This comment was posted automatically by a bot. All AutoModerator settings are configured by individual communities. Contact this community's Moderators to have your post approved if you believe this was in error.

/u/Witchman05 P roject Envoy

Nobody cares about who you are.

/u/TweakCity

/u/martinatchet Cumstain

now if this were envoy it'd be a different story...

/u/thierry05

We're all degenerates on here 'feds' don't care about us.

/u/TweakCity

Stop downplaying the situation.

You sound like a fucking cop.

I should of posted this in /d/opsec

/u/thierry05

my fellow degenerate this is what society calls a joke

/u/capobianco

No, he is right you fucking retard. There are too many people in here to focus on a particular person. The really popular people would need to be more wary but I am sure they already are.

/u/AutoModerator M Fuck You

well, i disagree but your thoughts are appreciated and valid, and will be taken into consideration. thanks for commenting.

This comment was posted automatically by a bot. All AutoModerator settings are configured by individual communities. Contact this community's Moderators to have your post approved if you believe this was in error.

/u/TweakCity

You need to keep up with society and how fast we're advancing in technology. You fucking retard. Go hit k-12 again. You got some catching up to do.

/u/AutoModerator M Fuck You

well, i disagree but your thoughts are appreciated and valid, and will be taken into consideration. thanks for commenting.

This comment was posted automatically by a bot. All AutoModerator settings are configured by individual communities. Contact this community's Moderators to have your post approved if you believe this was in error.

/u/capobianco

Bro, please shut the fuck up you're too motherfucking paranoid with shit. While yes Dread is a very popular site with a lot of vendors, buyers, and outlaws. No police officer would bother to try to decrypt and crack a person's information about someone. As we all know everyone (hopefully mostly) gives vague replies to their personal information. Now meanwhile if you are a vendor, I am sure they would understand the simple precautions of revealing minimal information about themselves, if they are international no information should be given at all honestly. The pigs will wander around dread but will not bother to find anyone unless the person very blatantly gives out their information which moderators would very carefully look into and try to delete; it's not certain. I find it very amusing how one could talk about such a big topic with minimal knowledge, if you said this on /d/opsec you would've gotten shatted on or perhaps even have your post removed by how brainfucking it is. If you do have any further questions or counterarguments please do reply to my comment, same goes for anyone viewing this post.

If you ever do decide to post on opsec, mention me as someone who counter-argued you and do quote this message as I am intrigued by the insight of further information.

/u/AutoModerator M Fuck You

"No matter how paranoid you are, what they're actually doing is worse than you can possibly imagine."

This comment was posted automatically by a bot. All AutoModerator settings are configured by individual communities. Contact this community's

Moderators to have your post approved if you believe this was in error.

/u/capobianco

Thank you Automoderator, yes the feds are indeed far worse.

Is Dread up and online on the DarkNet?

Check if Dread is online. Dread is a DarkNet forum built in the likeness of Reddit. It was founded by HugBunter after Reddit banned hundreds of communities in 2018.

darkfailenbsdla5mal2mxn2uz66od5vtzd5qozslagrfzachha-3f3id.onion

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv-7jicoxknyazubrad.onion

Hugbunter usually posts updates to a Reddit sub /r/dreadalert whenever the site experiences significant downtime.

For Example:

r/DreadAlert • u/hugbunt3r

[June 20th] DoS attack on-going

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA512

The original attacker who forced Dream offline back in 2019 and also took Dread down many times, before then disappearing later that same year, returned 2 weeks ago and has been attempting to extort us along with other markets. We are currently down and I am not in a position to scale things for a few hours, so expect downtime of at least 6 hours from the time of this post (5pm UTC).

We'll scale up when possible and all will be good, the worry I have is that a market is going to pay him so he can expand his attack. Unlike all of the copycat attacks that he has sparked since that point, ***his attack directly targets inefficiencies in the Tor protocol to overload hidden services and their guards,*** *rather than mainly overloading the application layer. This means his attack is extremely powerful and requires a lot less resources to accomplish, it is dangerous. Markets and other services he targets, will follow our guidelines as usual to recover, but there are still bottlenecks in the network which we can all hit when scaling. The main hope is that he doesn't receive funding to increase his fire power.*

If you've noticed Tor being extremely slow recently, it is possible that he is at least partially responsible. This is a reminder to any hidden service operator, never pay when being extorted, once they want more money they will always come back and you're funding him to do just that.

Dread has never and will never pay out to an attacker and we will never be forced to apply mirror addresses for more than a couple of hours, if ever.

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEEYTOs4fS4fFHb8/6l6GEFEPmm6SIFAmKwqUYACgkQ6GEFEPmm

6SIrERAAhXvEVlaj4ruQ+tEot2tSg3neSUxyHn86HnMr/rwF1BMNEMp6UV1daYzK

eGnwD1bCEA3K5DPhDbIo0hCfWqWMOwtV9dwBP4XOtQ6S3N5ggryqD3C9L1eboFrD

U9dG6Gg63aLByglu9Oay6p6gM8o8VXGHOXWO0hgeEKedC9kB5kZiuO+eow0x39LC

5SFVZ85DyDjjGULPhuHTg8cZ5PAVwTUWDyDAGeyG0ES1Gf1Uj4/gyP/oOmD+nKo+

1bSWujK/XykBeRtpD22OUNngcf3veuRgGyjsgqrOxmF0EZvFLV5VfKOu6oQYmZFn

A+8m6PaxsH2gXkYfRWxF+1coXw4s8WBb8j0pcYgAJgcmTwBys+Nkx1E9Vip2nOOD

QMmI7OSRz3bvg80rNZrHYwl2EUI+1XP34SG/Q3ZXf6fOSNtNoSaq7nn2BcC8cfm/

646CAXrjx0slCUd4sUJbQ0v+6YhuSAAHOdiQVTlXmGUAt1pkYi7Z9cnfiOAzdw1V

o0w28iJxSsE80pC7T7QzIpsxFZgyaQLI8qNr/HriN5qemONZsqybfRBqg8A1eStP

VqBo9PSd1U2wl1lMQgAgNnqng2PeSn5/VhONPShdgauL+PDVZWsMkwX47st7GKMS

zkq54AA8jHSEpuo1c53MM+IW0k6ThNNt5av0iEOrZ+bGk8i3t7o=

=y02h

-----END PGP SIGNATURE-----

u/Jayocarlow1986

Fuck!! ,, Thanks for all your hard work as always

u/ChrisButPrivate

Dread is still reachable on I2P

u/hugbunt3r

Ha I completed forgot

u/Hadrunken

What's I2P

u/ChrisButPrivate 17h ago

To keep it really short and simple: It's something like TOR but different. After you successfully configured I2P, you can access Dread with this link:

dreadtoobigdsrxg4yfspcyjr3k6675vftyco5pyb7wg4pr4dwjq.b32.i2p

u/bchemboy93 17h ago

Down on i2p also

EDIT: it's loading, just congested traffic.

u/fuxnet 23h ago

ole gustav screeching again?

u/hugbunt3r

Gustav was not the original attacker

u/quoteFlairUpunquote

I wish there was a place to learn dark web history, so much of this stuff flies over my head

u/hugbunt3r

A lot of market history and archives of past markets and forums is available at Gwern.net, everything since February 2018 you can find documented in all historical posts from Dread. Of course, when the site is back online.

u/Potato2trader

What does the site operators do in such scenarios? Are they just waiting for the storm to pass or are there special techniques to deal with these bad actors.

When he talks about scaling to overcome this. What does that mean?

He also mentioned that he hopes the bad boy doesn't get funding to increase his fire power? What kind of power?

Excuse my noobnes.

u/hugbunt3r 17h ago

Scaling refers to increasing the amount of gateway servers which host the DoS captcha screen before proxying you through to the backend application (Dread). The more of these, the more traffic can be handled not only at the application layer, but over Tor. When you connect to the Dread onion address, you are actually connecting to one of many of these gateway servers that are under a different onion address, but there's no way to discover these addresses. They are essentially hidden behind the public onion address you are visiting. To achieve this we use software called OnionBalance, which is designed for load balancing of hidden services.

To explain the benefits to this, if you were to just setup a hidden service in a standard way, that is one Tor process running which every user's circuit is handled through. If this Tor process is overloaded then the service becomes unreachable. Using OnionBalance, you now have multiple Tor processes accessible via the single onion address, which spreads the load between them, as long as one of them isn't completely overloaded, the site will be accessible. So if you scale this with lots of new servers, your ability to withstand an attack improves massively. This is simplifying it to some extent and there are other issues with the Tor network (bottlenecks), which can still prove to be difficult to overcome and your hidden service remains unreachable.

u/quoteFlairUpunquote

Where can I learn about this?

u/hugbunt3r

Checkout the /d/EndGame subdread on Dread, where we released the

open source DoS captcha module. Ideal setups are discussed for OnionBalance.

u/KaptainSynchro

Thx for the update-was wondering what was up

u/Tombstonesss

thanks for the update

u/drupe14

Thanks for the update!

u/mjck77

Thanks for the update Hugbunter.

u/Additional_Egg8307

Thanks for the update. This shit is so Fucking whack

u/SalamanderMost8744 11h ago

Anyone suspicious this is actually the fbi?

u/[deleted] 11h ago

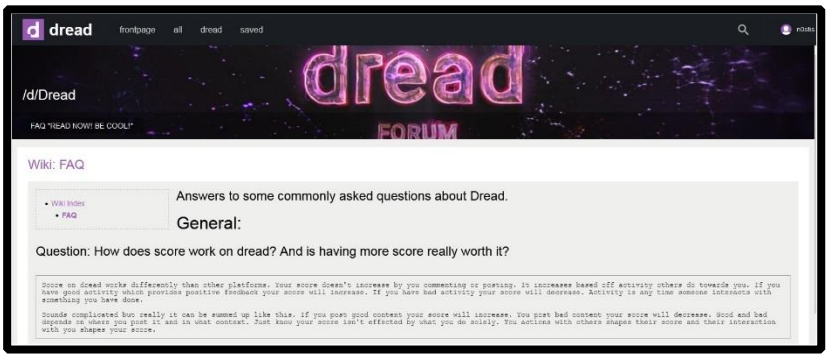
[deleted]

u/SalamanderMost8744 10h ago

You dum

Read the dread Frequently Asked Questions (FAQ)

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv-7jicoxknyazubrad.onion/d/Dread/wiki/?id=0f0519ab

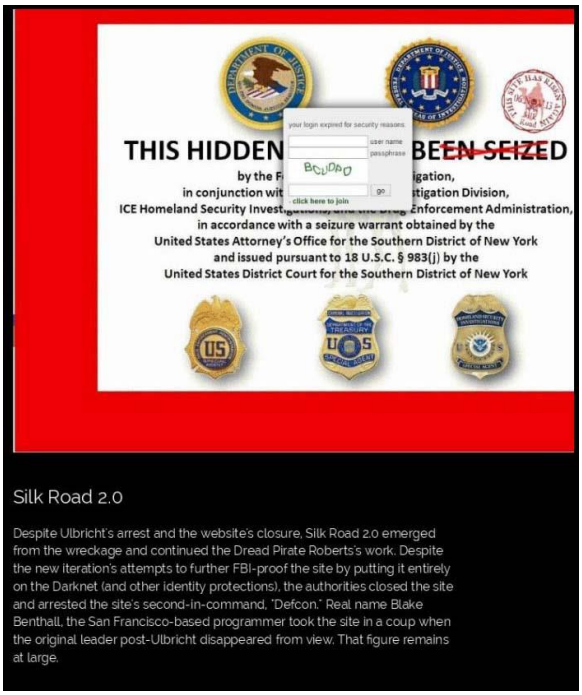


I did not plan on buying anything or dealing with purchasing materials or services using cryptocurrencies so I ignored most of this advice from the DarkNet Markets Buyer's Bible (DNM Bible).

Welcome to the DNM Buyer's Bible (DNM Bible) /d/dnmbible

http://biblemeowimkh3utujmhm6oh2oeb3ubjw2lpgeq-3lahrfr2l6ev6zgyd.onion/

Some DW sites get taken down.

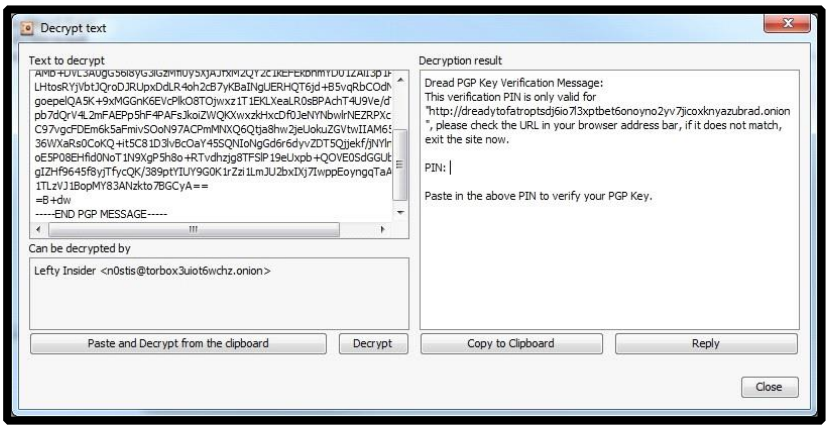

THIS HIDDEN
BEEN SEIZED
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York
Silk Road 2.0
Despite Ulbricht's arrest and the website's closure, Silk Road 2.0 emerged from the wreckage and continued the Dread Pirate Roberts's work. Despite the new iteration's attempts to further FBI-proof the site by putting it entirely on the Darknet (and other identity protections), the authorities closed the site and arrested the site's second-in-command, "Defcon." Real name Blake Benthall, the San Francisco-based programmer took the site in a coup when the original leader post-Ulbricht disappeared from view. That figure remains at large.

For The Newcomer | The Purpose Behind PGP Encryption & Cryptography

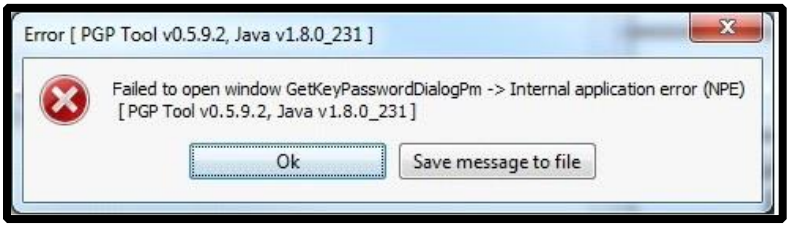
http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv-7jicoxknyazubrad.onion/post/e8d080f49b58545cb5a1

To receive encrypted messages on dread, you will need to put your PDP key into your profile.

Dread then sends you a message to decrypt and provide verification pin.



PCP Tool thru an unknown error but it worked anyway.


Error [PGP Tool v0.5.9.2, Java v1.8.0_231]
Failed to open window GetKeyPasswordDialogPm -> Internal application error (NPE)
[PGP Tool v0.5.9.2, Java v1.8.0_231]
Ok
Save message to file

OpSec /d/OpSec

Discussion of OpSec, Threat Models, Protection, Assessment & Countermeasures.

/d/OpSec

15,159 subscribers

http://dreadytofatroptsdj6io7l3xptbet6onoyno-2yv-7jicoxknyazubrad.onion/d/OpSec

While the focus of this community's OpSec discussions may center around Dark Net (DN) activity, all members of this sub are encouraged to think about, discuss, and share ideas relating to OpSec that extend beyond the bounds of the DN.

Wiki: Canary

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv-7jicoxknyazubrad.onion/page/canary/

Example Canary

This warrant canary page serves as a method of I, HugBunter, communicating with all users of my services to provide a regularly published PGP signature, verifying that I am alive and free as of the published date within the signed message. This will help to serve as disclosure if the server is compromised, or if anything has happened to myself. My PGP key is available on my profile at /u/HugBunter and should be stored by everyone immediately as this could be maliciously changed at any point in time.

The canary message will be consistently updated every Monday and will always include the current date. If the signature ever fails to verify, attempt to raise the alarm through any of my provided services and other popular channels, since it could easily be censored on any compromised service. Please allow no longer than 72 hours following each Monday if there hasn't been an updated signature published, which should account for any issues with me accessing to provide an update on the set day.

Because I am useless, this canary is often updated on Tuesday or Wednesday, my bad.

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

I, HugBunter am alive and free as of Tuesday, March 22nd 2022 and in full control of Dread, Recon and all other services related to our network.

Next canary update is scheduled for Thursday, March 31st 2022

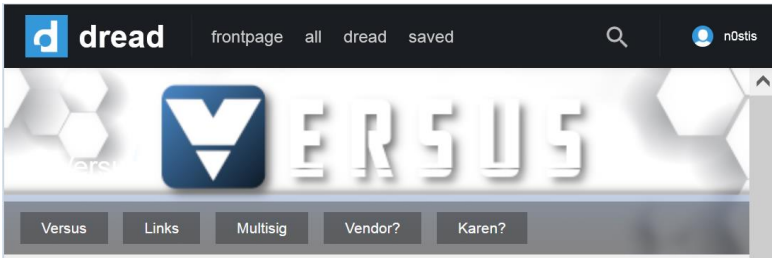
000000000000000000561de6ffa1624cabb82d101c8cea16ffb0079496b8fe8

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEEYTOs4fS4fFHb8/6l6GEFEPmm6SIFAmI5rIkACgkQ6GEFEPmm
6SLORRAAg130ufd3X1//RUGK+v9m/kxUieaLCSE5A6xjcuapWsfhOJVKH5AOH03q
VZCf4e79i8U4WphpfHMdM81x+zvtxZh0Q+OgumEC9rQXmHeRUZl/mIsdo3Yq3cHE
H9ljQLKlam+WVadW4mbSWLb0Bu7KJhtnt0530zClzgPQPpOo9wNmT1rSYGXHTySn
55WCmzsEWL4CSGKhqclDnIAaK8mvKEgs0rRK/XauiBBrn9PfzJU8Ldxne01tpLMa
NNyWiTV6WG9rNHNkqeM18cFQF4mCApYEQCY9C7qh59EgkWt2dTtlZZmmzNcYXPwH
UskEog5/NAhFUuOhO+r2rOOqGi7zp+tJ+TAPG0H9uPJwr8ZcArBAJ1wZV/ub7v08
jTCgMi5wSGy2gJjzvhk437JdD1WfNHLkA0SJPxs8VtyUVifR0lwqn4uCMrusY8fi
XTtkaa3lcd3zMaDfj0CSBHSs9MAnB2JKMGYw0lVrWIriI/xFf/SPnP1LMalkWKZu
NzGkHz/BWprCgk3VHkox8XhCou/gXK7AlAQNNmYS5qS0OGwFqWN04e7Gyen5yz/R
s5NsCI5KGgDCkxTFjEuvGS/ZH5IxoIpM2Oa7mv3eHp1jkFjcbEQU921Ih/ZDmhs7
7imrhZYV5HfBqeVol4EgiHaSUFpT+DO195sm+h3ndf+rP1+eeDw=
=fs3t

-----END PGP SIGNATURE-----

Apparently this is a submarket within dread. The following does provide some insights as to how these markets work, or don't.



http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv-7jicoxknyazubrad.onion/d/Versus

That's all, folks!

by /u/WilliamGibson ✶S TΛ F F ✶ • in /d/Versus

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA512

Dear community,

Due to the huge influx of user, the even bigger influx of complete retards and the therefor inevitable decline of our support quality in the recent month we decided to close our registration and convert the market into a private community to keep our quality standards up and idiots out. We never intended to be the #1 Market but here we are. It is time to get back to the roots. We always wanted to provide a high quality platform for the community and that is where we are heading again. We prefer quality over quantity. While the recent influx is nice for our wallets we don't want to become the next Empire-esque shitmarket.

>What does this mean for new buyer?

Well you are out of luck if you don't have an account yet. We will soon enable vendors to give out invite codes. Ask your vendor for an invite code to register an account on Versus or wait until we periodically open up registration for a limited time.

> What does this mean for vendors?

We will personally invite you if we believe you are a good match for the community. We don't accept any more applications or vendor bonds. All existing vendors will be able to give out a limited amount of invite codes per week. Those INVITE CODES ARE NOT FOR SALE. We will monitor invites and if we believe you are selling them on other markets we will ban your account.

Going invite-only is a necessary step to keep our quality standards up.

The quality of our vendor, of our buyer and our own staff and support.

Have a nice trip, William Gibson

-----BEGIN PGP SIGNATURE-----

iQKTBAEBCgB9FiEEFAl5ki+ljOnGotMlXFDURnuuQqEFAmJ0X6tfF IAAAAAALgAo

aXNzdWVyLWZwckBub3RhdGlvbnMub3BlbnBncC5maWZ0aGhvcnNl bWFuLm5ldDE0

MDk3OTkyMkZBNThDRTlDNkEyRDMyNTVDNTBENDQ2N0JBRTQ yQTEACgkQXFDURnuu

QqG+Bg//ckGuZJPaaoecDPR+zdgkELno+bLoDL3IyT7nHf1DJ7HgW CGbbSdNBuK/

Uj+5ns/QCge8KsyWlxIJyiNiY3Rkz64zxb7c9lM1vUoO8KnPMNskcV3v all82L06

hcz8+uGWBJUtw9H45W3t4d3VwpQ9WHqTIqW/4PSyiFjdJkbmWKk HwvMF5qRTILsN

PXAI6qa3C1FpfH25CjhoK7PgUqyXZyr0wXNVoIi0+bXpc/YBr97fvnD EJLH2rMpv

9CyxTIJXz9WKxrueVB3OTzXNXeUAm8iAS1SV/c9Vs5NUgMSLx946 AzlKKJxscLHp

741EA/2h+xY48Rr3bjUQe3ur0rFCTvGkq63WQCFR38dhRvCCwP09+ omwgW68Bz8s

hT8qK/trG6CsjjN9+t+EIgr6hsPtRydBIN1njpamsQWB0eMfF/icO7ybZ QQZ853J

yp0f41YtczSzXvM1SKRthPsWAZ6s2KkjAFyBwrbPeraOSXroqjVa/tp+ AwVndALA

YKe3NglQ92ZN+uwPZQn7ySNT3HqZw4hOjNJ/vg7kzLbjSIJwxx3uX JbWCJ7meV5R

kIO9oQgpWCjuy6wBz+heiq9svCS/7yfYzTUq1mbJB9oO9PKR5jLB+d5 WWjHozHHY

ZjoRBB0y4pV7qdgUNiiwok8DD43IF8pRkscrEo6qbWBBJYcA/BE=

=Nypb

-----END PGP SIGNATURE-----

Then a clarification to a user:

/u/Pineapplegod69

To be fair, I kinda feel like one of the complete retards after the multi sig refund I got confused with, I eventually figured it out. Quite happy I have an account & really like this idea going forward.

/u/WilliamGibson ✶S TΛ F F ✶

I can assure you that you are not one of them. When I talk about complete retards I don't refer to user who just don't know how things work but to user who who think they know it all and act accordingly. There is absolutely nothing wrong with not knowing. We are happy to help wherever we can. When I talk about complete retards I mean the type of user who think WE (the

market) is sending out any product. The type of user who threatens to kill us because they got phished. The type of user who thinks this is Amazon. The type of user who believes creating drama on dread will resolve his issues sooner. The type of user who thinks he doesn't need to read anything and the whole world only exists to spoon feed him. There are a lot more retards but I can assure you that you are of one of them if you just don't know everything. There is no shame in not knowing. We all have to start somewhere.

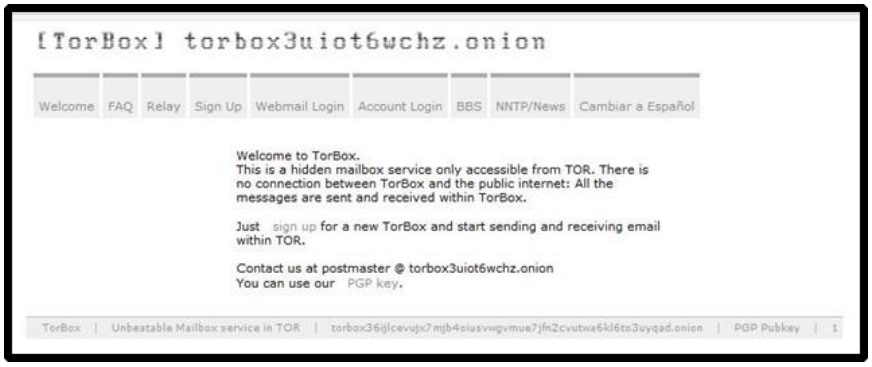
Dark Web Email

TorBox Email

http://torbox36ijlcevujx7mjb4oiusvwgvmue7jfn2cvutwa-6kl6to3uyqad.onion

TorBox is a hidden mailbox service only accessible from TOR. There is no connection between TorBox and the public Internet: All the messages are sent and received within TorBox. You just need to sign up on their website and start sending and receiving emails anonymously.

Note: Currently, TorBox supports emails to and from lelantos.org, maskedmail.com, mail2tor.com, mailtor.net and safe-mail.net.

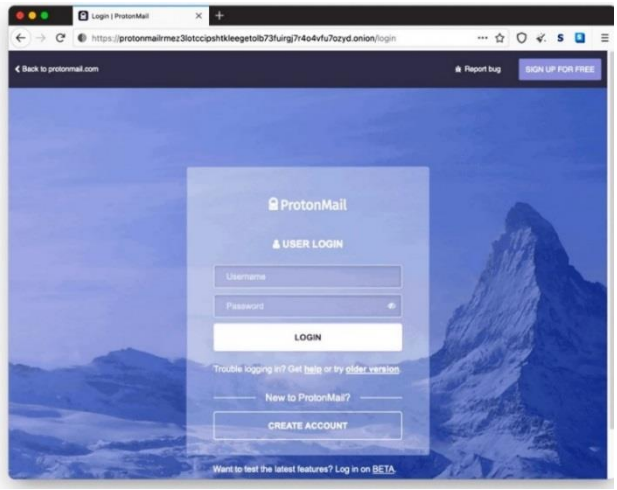

[TorBox] torbox3uiot6wchz.onion
Welcome
FAQ
Relay
Sign Up
Webmail Login
Account Login
BBS
NNTP/News
Cambiar a Español
Welcome to TorBox.
This is a hidden mailbox service only accessible from TOR. There is no connection between TorBox and the public internet: All the messages are sent and received within TorBox.
Just sign up for a new TorBox and start sending and receiving email within TOR.
Contact us at postmaster @ torbox3uiot6wchz.onion
You can use our PGP key.
TorBox | Unbeatable Mailbox service in TOR | torbox36ijlcevujx7mjb4oiusvwgvmue7jfn2cvutwa6kl6to3uyqad.onion | PGP Pubkey | 1

ProtonMail

https://protonmailrmez3lotccipshtkleegetolb73fuirgj-7r4o4vfu7ozyd.onion/

Based in Switzerland, ProtonMail is an encrypted email service that is very popular with cryptocurrency enthusiasts. It is not free, but it is extremely secure.

ProtonMail was initially conceived at CERN, the European Organization for Nuclear Research, where the World Wide Web was created.



Proton requires Javascript. Enable Javascript and reload this page to continue.

Note: This may be a deal breaker for some.

2021, Proton, Proton logged IP address of French activist after an order bySwiss authorities.

TechCrunch, Proton logged IP address of French activist after order by Swiss authorities.

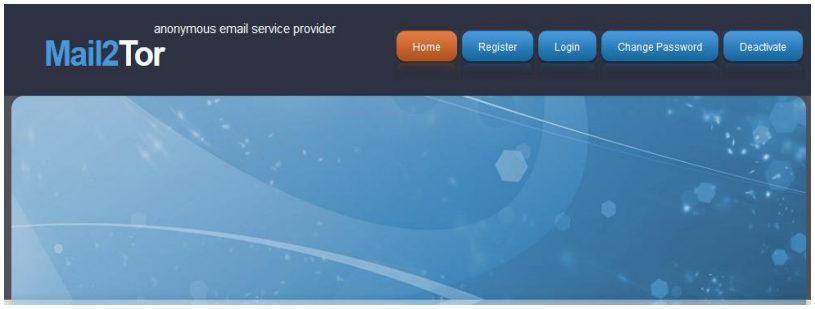
https://techcrunch.com/2021/09/06/proton-logged-ip-address-of-french-activist-after-order-by-swiss-authorities/

Web creator Tim Berners-Lee joins ProtonMail's advisory board

https://www.zdnet.com/article/world-wide-web-inventor-berners-lee-joins-protonmails-advisory-board/

Mail2Tor - Anonymous Email Service Provider

http://mail2torjgmxgexntbrmhvgluavhj7ouul5yar-6ylbvjkxwqf6ixkwyd.onion/



Mail2Tor Onion Page

Mail2Tor is a free anonymous e-mail service to protect your privacy. It allows anyone to send and receive email anonymously via webmail or with an email client. You will need to have Tor browser installed on your computer to access Mail2Tor.

IMAP Address:

g77kjrad6bafzzyldqvffq6kxlsgphcygptxhnn-4xlnktfgaqshilmyd.onion:143

SMTP Address:

xc7tgk2c5onxni2wsy76jslfsitxjbbptejnqhw6gy2ft-7khpevhc-7ad.onion:25

We do not use TLS/SSL

For help...contact admin@Mail2Tor.com. Change your password by yourself. Deactivate your account by yourself too. All messages are stored in encrypted form. In the headers of your emails will not appear your IP number. We will add more servers soon. All problems kindly reported by users will be solved. Be patient, please.

We have been receiving a number of emails regarding forgotten/invalid password. Do note that by virtue of the setup we are unable to verify your identity and hence unable to aid in this matter. Do try not to forget your password. We will not allow reset/hijack of accounts for the privacy and safety of all.

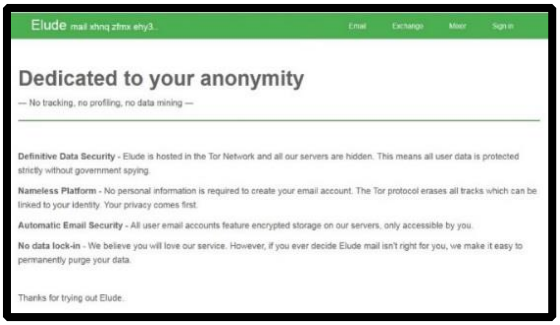
Elude

If you are looking for a no-frills email service provider that is exactly the opposite of Gmail, Elude is there for you. It is free, does not bombard you with ads, and does not track you with Google Analytics or the like. You will get an email address free. No personal information is required to create your email account and all email accounts are encrypted and stored in their hidden servers. .onion link: The only correct .onion address for Elude is:

http://eludemailxhnqzfmxehy3bk-5guyhlxbunfyhkcksv4gvx6d3wcf6smad.onion/

elude
Due to on-going DDOS attacks against our servers, you must complete a captcha challenge to prove you are human.
VERIFY
Select only color filled symbols:
Empty symbols should not be selected:
All correct symbols are in a horizontal line

Solve CAPTCHA to enter


Elude
Dedicated to your anonymity
— No tracking, no profiling, no data mining —
Definitive Data Security - Elude is hosted in the Tor Network and all our servers are hidden. This means all user data is protected strictly without government spying.
Nameless Platform - No personal information is required to create your email account. The Tor protocol erases all tracks which can be linked to your identity. Your privacy comes first.
Automatic Email Security - All user email accounts feature encrypted storage on our servers, only accessible by you.
No data lock-in - We believe you will love our service. However, if you ever decide Elude mail isn't right for you, we make it easy to permanently purge your data.
Thanks for trying out Elude.

The reviews are not good, primarily due to the service being down more that up.

List of email providers

- ProtonMail – protonirockerxow.onion, ClearWeb
- TorBox – torbox3uiot6wchz.onion
- Bitmessage – bitmailendavkbec.onion, ClearWeb
- Mail2Tor – mail2tor2zyjdctd.onion
- RiseUp – nzh3fv6jc6jskki3.onion, ClearWeb
- Cock.li (NSFW) – cockmailwwfvrtqj.onion, ClearWeb
- Lelantos – lelantoss7bcnwbv.onion paid accounts only
- Autistici wi7qkxyrdpu5cmvr.onion ClearWeb https://autistici.org
- AnonInbox – ncikv3i4qfzwy2qy.onion paid accounts only
- VFEMail – 344c6kbnjnljjzlz.onion, ClearWeb
- **Dead:** Sigaint – sigaintevyh2rzvw.onion
- ane-mail address from these providers:
- MailFence:https://mailfence.com/
- Disroot:https://disroot.org
- Envs.net:https://envs.net/

Tutanota

Tutanota is the world's first end-to-end encrypted mail service that encrypts the entire mailbox. With its unique open source technology Tutanota fights for privacy and freedom of speech online. Started as a secure email service in 2011, Tutanota now offers an encrypted address book, an encrypted calendar and the encrypted contact form Secure Connect.

In addition, Tutanota's affordable business version enables companies and organisations of all sizes to easily secure their email communication.

https://tutanota.com/ https://tutanota.com/about

Note: requires JavaScript

2021, The Germany-based mail provider Tutanota was forced to monitor specific accounts for 3 months.

2020, The Germany-based mail provider Tutanota was forced to implement a backdoor to intercept and save copies of the unencrypted e-mails of one user285(they did not decrypt the stored e-mail).

Court rules encrypted email provider Tutanota must monitor messages in blackmail case.

https://www.cyberscoop.com/court-rules-encrypted-email-tutanota-monitor-messages/

Secmail

Email security

Protects organizations from cybercrime and saves employees' time by blocking harmful and unwanted emails.

SecMail® is a comprehensive and unique email spam prevention service. It also encrypts and protects the user company's email traffic and servers. In addition to tackling common junk email and viruses, SecMail® allows users flexibly define their own guidelines in blocking all unwanted email traffic such as marketing emails and advertisements.

Unlike a number of somewhat similar services SecMail® Email Security isn't just an email filtering service. SecMail® actually detects

and blocks the spam already in the transmission process and then utterly prevents the receiving of them. Hereafter, typical email servers return the email back to the sender followed by a delivery block message with SecMail®'s error description. The service user can also check the blocked messages from SecMail®'s easy to use interface and, furthermore, simply release messages.

Blocked emails

SecMail® Email Security system immediately informs blocked email senders about the blocking with an error description. The error is presented as delivery status information of the used mail protocol (SMTP), which any properly functioning email program will deliver to the sender of the blocked email.

https://Secmail.com

Secmail.Pro

Free email provider with anonymous sign up and PGP encryption, the service is widely used by various dark market users. Unfortunately it cannot receive email from Gmail, Yahoo and other major providers as their servers are marked spam, Secmail claims to be working on a proxy system to solve this.

The domain name
Secmail.pro
May be available for sale
This domain name (without content) may be available for sale or lease by its owner through Bodis's domain sales platform.

https://sigaintevyh2rzvw.onion

Invalid Onionsite Address. Go figure. And so it goes on the Dark Web.

Juvenile - No Rules

https://infantile.us/

The deep web starts right here!

This is an introduction point to the deep web for any who are interested. The deep web is a protected part of the internet, and you must use special software to use it. While this software is commonly known by many, most do not know many hidden services to reach using it. Juvenile is here to be your first step in a journey that is being taken by many. These steps are leading mankind to a new age and a new era.

If you follow the instructions below you will find the hidden service version of Juvenile. From there you will find a list of links that should get you started on your journey.

The onion domain below is available through the Tor network...

https://juvenilezskkwc2gu7j5c4akppjnr3kzlgljjeodd-5psn-6fwcnloplid.onion

This service has developed from being Infantile to being Juvenile!

The name has nothing to do with sexy teenagers.

Links to other Onion sites

Secure Email

Infantile offers an exclusive mail service only for the dark web's best and brightest. Use the contact details for kaizushi below if you think that is you.

If you are accepted accounts cost only $50 a year, and must be paid in XMR.[15]

Contact Kaizushi
You can contact me by email on kaizushi@infantile.us
You can contact me by XMPP on kaizushi@infantilefb6ovh4.onion
(this requires an account on the same server)
You will find keys on my KLOS contact page.

Subject: *Infantile mail*
From: *"Kaizu Shibata" <kaizushi@infantile.us>*
Date: *Mon, June 13, 2022 2:39 am*
To: *n0stis@mail2tor.com*

Your background looks pretty solid, I charge $50 USD a year for an Infantile mail account.

Shall I generate an invoice for you to pay?

Kaizu Shibata
<kaizushi@infantile.us>
Kaizushi's Little Onion Server
https://kloshost.online/
kaizushih5iec2mxohpvbt5uaapqdnbluaasa2cmsrrjtwrbx46cnaid.onion

Subject: *Infantile mail*
From: *n0stis@mail2tor.com*
To: *Kaizu Shibata" <kaizushi@infantile.us>*

So I am playing with free Mail2Tor and Sector.city now.

Tell me why I should pay you before I even see or use your service?

Do you have a trial period?

n0stis

Subject: *Re: Infantile mail*
From: *"Kaizu Shibata" <kaizushi@infantile.us>*
Date: *Tue, June 14, 2022 1:04 am*
To: *n0stis@mail2tor.com*

Sector only supports webmail and has limits on how many messages can be sent from it a day.

Mail2tor also has limits that are required of a free service that anyone can use to prevent it being abused.

---

[15] *Monero (Abbreviation: XMR) is a decentralized cryptocurrency. It uses a public distributed ledger with privacy-enhancing technologies that obfuscate transactions to achieve anonymity and fungibility. Observers cannot decipher addresses trading Monero, transaction amounts, address balances, or transaction histories.*

An Infantile mail account has far less limits than these providers, and because I curate potential users one can trust mail from my domain more than other providers.

Kaizu Shibata
<kaizushi@infantile.us>
Kaizushi's Little Onion Server
https://kloshost.online/
kaizushih5iec2mxohpvbt5uaapqdnbluaasa2cmsrrjtwrbx46cnaid.onion

Ok, so that is a sales pitch not answers to my questions. So this is a big fat no thanks from me.

Private email you can trust

We protect your data, activity, and privacy with state-of-the-art security and technology.

https://www.startmail.com
Personal Private and encrypted email
$5 $2.50 per month, billed annually*

We are located in the EU, and we fully comply with applicable privacy laws and regulations of the EU, including the General Data Protection Regulation (GDPR). These are widely regarded as the strongest privacy protections in the world.

Top 5 Dark Web Email Providers (another list)

ProtonMail.com

protonirockerxow.onion

While it may seem odd that a non-dark web exclusive email provider would be number one on the list, ProtonMail has rightfully earned their spot with notable security measures and an HTTPS secure dark web portal. ProtonMail has made its way to the top of the list for the extensive security measures they employ across their network. The only downside to ProtonMail is you cannot register with a .onion address, making all emails default ClearWeb domains.

ProtonMail does enforce several security measures to make up for the ClearWeb domain. For beginners, everything on ProtonMail is end-to-end encrypted, a method that allows only a single end-user to see the contents. With all contents being end-to-end encrypted, only you can see your email. On top of this, ProtonMail ensures that they run their emails in a zero-knowledge environment. Meaning even if they wanted to read your communications, they would not physically be able to, only you can unlock the encrypted contents.

ProtonMail is not only secure on the software side but on the hardware side as well. For one, ProtonMail operates out of the jurisdiction of Switzerland, a country with some of the strongest privacy laws throughout the globe. Not only do they operate out of Switzerland, but they also own and operate all their own hardware. According to ProtonMail, they use strictly dedicated servers they own at select data centers scattered throughout Switzerland. No VPS or shared servers, ProtonMail strictly employs dedicated hardware in the country they operate out of.

Highlights:

- Everything end-to-end encrypted
- Zero-knowledge
- Dedicated hardware
- Operates out of the jurisdiction of Switzerland

- Symmetric encryption for seamless secure communication
- Free

Downsides:

- Only Clearnet @protonmai.com emails.

One last great feature about ProtonMail is they allow you to easily send encrypted emails to other secure email providers through symmetric encryption. Allowing you to communicate with others using secure email without having to worry about the Clearnet or go through the hassle of manually encrypting everything. Lastly, they enforce HTTPS on their .onion domain, a rare technique that is perfect to ensure you always visiting the official ProtonMail dark web domain.

One upside and downside to ProtonMail is the owners are not anonymous, and they do operate a real business. ProtonMail won't just fail and instantly fall dark like a lot of dark web providers have done in the past. While there are many benefits to the owners remaining anonymous, it can be a huge burden if the company simply decides to pull its plug. To ensure your always visiting the official ProtonMail dark web website, refer to their Tor page on their ClearWeb domain: protonmail.com/tor

ProtonMail Unifies Encrypted Mail, Calendar, VPN, and Storage Services Under New 'Proton' Brand (macrumors.com) 34

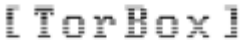
Posted by msmash on Wednesday May 25, 2022 @02:44PM from the closer-look dept.

Swiss-based encrypted email provider ProtonMail today announced a restructuring of its privacy-first services, bringing them under a new unifying brand name: Proton. "Today, we are undertaking our biggest step forward in the movement for an internet that respects your privacy. The new, updated Proton offers one account, many services, and one privacy-by-default ecosystem. You can now enjoy unified protection with a modernized look and feel. Evolving into a unified Proton reflects our growth from an end-to-end encrypted email provider to an entire privacy ecosystem, allowing us to deliver even more benefits to the Proton community and make privacy accessible to everyone," the company said. MacRumors adds: Previously, users could only subscribe to each service the company offered individually. Going forward, the new Proton offers one account to access all the services offered in the company's privacy-by-default ecosystem, including Proton Mail, Proton VPN, Proton Calendar, and Proton Drive, all of which can be accessed from proton.me. All Proton services remain available as a free tier, with more advanced features and more storage available via paid plans. The free Proton tier includes up to 1GB of storage and one Proton email address, as well as access to Proton's encrypted Calendar and VPN services. ***Further reading****:*

Proton Is Trying to Become Google -- Without Your Data.

TorBox

torbox3uiot6wchz.onion



A rather simple provider is TorBox, a TOR-only service. This means that no ClearWeb connections are made, making this email **darkweb exclusive**. If the recipient isn't using a TorBox-certified provider, the email will not be sent, even if it's darkweb compatible. *Currently, TorBox supports emails to and from lelantos.org, maskedmail.com, mail2tor.com, mailtor.net and safe-mail.net.*

TorBox is a strictly Tor email and has no intention of releasing a ClearWeb friendly service in the near future. TorBox is 100% free and offers 25 megabytes at signup and offers more disk space for bitcoin donations. All email data stored on servers is encrypted due to the server itself using encrypted partitions.

As the name suggests, TorBox is a Tor-exclusive email, where no packet or email header will ever hit the ClearWeb.

Bitmessage

http://bitmsgdyvsmwgsimkxplisxbzpewvkhfm3fmomzd63apaymaxiznz-6ad.onion/

Bitmessage is another free, Tor-friendly, and privacy-conscious email provider. Throughout the domain, Bitmessage employs zero type of tracking or advertisements. Though they do collect a few stats about the service including the number of active users, the number of emails sent, the number of emails received, and few server logs (IMAP, SMPT, etc.) though none of this information is ever personally identifying.

For security Bitmessage employs a transport system that runs inside a sandbox, disallowing information to leave except through previously defined channels. The data on disks is encrypted and emails are actually deleted from the system when you delete them from your account. While the service is Tor-friendly it is not Tor-exclusive and allows you to not only connect but send and receive messages through both their ClearWeb and dark web portals.

However, one downside is they require you to verify with a google-owned captcha service on their signup page. Other than that all content is locally hosted.

Bitmessage is a P2P communications protocol used to send encrypted messages to another person or to many subscribers. It is decentralized and trustless, meaning that you need-not inherently trust any entities like root certificate authorities. It uses strong authentication which

means that the sender of a message cannot be spoofed, and it aims to hide "non-content" data, like the sender and receiver of messages, from passive eavesdroppers like those running warrantless wiretapping programs. https://bitmessage.org/bitmessage.pdf

Mail2Tor

And the last free service making our top 5 dark web email providers is Mail2Tor, another Tor-exclusive email.

Mail2Tor is only accessible via the Tor network but can both receive dark web and ClearWeb emails, making this another dual compatible setup. The site is quite minimalist and doesn't provide a whole lot of information outside of it being a Tor-only email provider. The service has been around for quite a while and has served the Tor community well during its time.

Mail2Tor (new onion)

https://mail2torjgmxgexntbrmhvgluavhj7ouul5yar6ylbvjkxwqf-6ixkwyd.onion

All system up. Fixed config error when trying to login SquirrelMail.

All mails is restored. New SSD to make server faster.

Spam assassin for incoming and limits to outbound emails count are imposed.

90 days old email auto deleted.

Only ONE admin -> admin@mail2tor.com
Please make Donation to 18iX81J8LYiTZyC1xJdw26pnYBFtsEX9hL
Any amount is not small.

Cock.li

cockmailwwfvrtqj.onion (NSFW)

While the name might sound like the most serious email provider, it's not, but one thing they do care about is privacy. Cock.li is run by an individual who owns a number of NSFW domains and decided to make it an email provider. Be warned, the domain may not be safe for work if others are around.

While it's a silly name, it is a very real email provider and about as transparent as they come. Cock.li advertises itself as an email ran by "some dude", not a business, and that does come with its own set of perks. One of those being complete transparency, or about as clear as they come. For starters, the owner of Cock.li, who we'll refer to as Vincent Canfield from now on, has the total monthly costs listed on the homepage. Right under that, Canfield has a transparency report, publishing all the legal documents he receives and information he is ever forced to disclose.

Alongside transparency, he also provides a DarkNet portal, https://cockmailwwfvrtqj.onion, and clearly outlines how his webmail runs. Letting everyone know that email is inherently insecure and how he technically does have the ability to read emails, just like nearly any other provider. While all of this may sound a little scary, Cock.li is a very well respected email provider among regular dark web visitors.

Others

This is a suggestion from a dread message. Judge for yourselves, but this has got to be one of the ugliest onion site I have ever seen.

/u/SamSpade2

saw ure post on the email thread i was also looking at better email providers than elude. who do u use

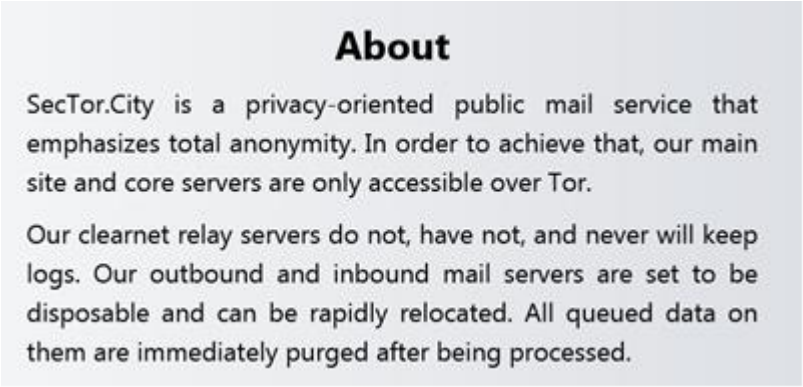
check this out

EMAIL SOLUTION SHADOW WIKI

- *http://abrx6wcpzkfpwxb5eb2wsra2wnkrv2macdtkpnrepswodz5jxd4schyd.onion/email.xhtml*

Another suggestion in a dread message. Judge for yourselves.

Sector.city is a very minimalist service with a ten email limit per day.


About
SecTor.City is a privacy-oriented public mail service that emphasizes total anonymity. In order to achieve that, our main site and core servers are only accessible over Tor.
Our clearnet relay servers do not, have not, and never will keep logs. Our outbound and inbound mail servers are set to be disposable and can be rapidly relocated. All queued data on them are immediately purged after being processed.

http://sector2nyjrxphgrj3cvnueanomz4trvgyxofvu-3cexltoxuegtlmzid.onion/

So this is not a plus to this service.

Subject: Undelivered Mail Returned to Sender
From: "Mail Delivery System" <MAILER-DAEMON@mail2tor.com>
Date: Tue, June 14, 2022 2:31 pm
To: n0stis@mail2tor.com
The mail system <n0stis@sector.city>:
connect to mail.sector.city[185.243.112.202]:25:
Connection refused

Conclusion

When dealing with email on the dark web you need to be extremely cautious as email is a serious service that needs to be properly handled. If your communications fall into the wrong hands it can be critical and can even cost some people their lives in other countries.

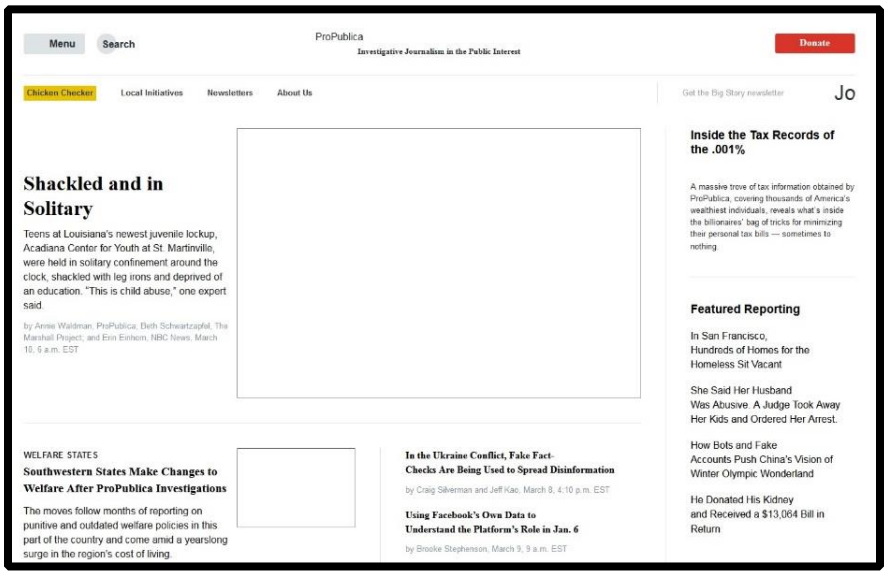
Email privacy is a serious concern and should not be taken lightly. Your inbox holds not only your common interests but extremely private information, and if you're working on the dark web, it's presumably even more sensitive. And finding a provider that can offer secure communications is something hard to trust, especially when working on the dark web as many government agencies want to de-anonymize Tor users.

While the Tor Project continues to battle the waves of government these are some emails that can combat mass surveillance as well. Ensure that you keep up your operational security (#OpSec) on high defense at all times when using any dark web email provider.

Dark Web Onion News Sites

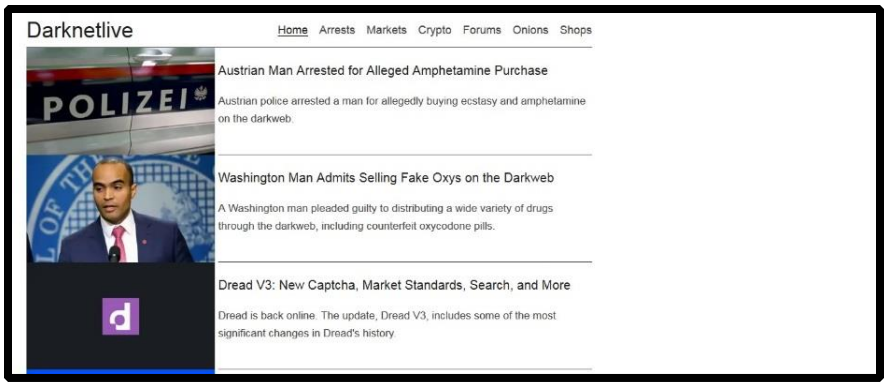
ProPublica

p53lf57qovyuvwsc6xnrppyply3vtqm-7l6pcobkmyqsiofyeznfu5uqd.onion


Menu
Search
ProPublica
Investigative Journalism in the Public Interest
Donate
Chicken Checker
Local Initiatives
Newsletters
About Us
Shackled and in Solitary
Teens at Louisiana's newest juvenile lockup, Acadiana Center for Youth at St. Martinville, were held in solitary confinement around the clock, shackled with leg irons and deprived of an education. "This is child abuse," one expert said.
Inside the Tax Records of the .001%
A massive trove of tax information obtained by ProPublica, covering thousands of America's wealthiest individuals, reveals what's inside the billionaires' bag of tricks for minimizing their personal tax bills — sometimes to nothing.
Featured Reporting
In San Francisco, Hundreds of Homes for the Homeless Sit Vacant
She Said Her Husband Was Abusive. A Judge Took Away Her Kids and Ordered Her Arrest.
How Bots and Fake Accounts Push China's Vision of Winter Olympic Wonderland
He Donated His Kidney and Received a $13,064 Bill in Return
WELFARE STATES
Southwestern States Make Changes to Welfare After ProPublica Investigations
The moves follow months of reporting on punitive and outdated welfare policies in this part of the country and come amid a yearslong surge in the region's cost of living.
In the Ukraine Conflict, Fake Fact-Checks Are Being Used to Spread Disinformation
Using Facebook's Own Data to Understand the Platform's Role in Jan. 6

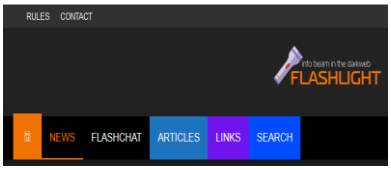
Darknetlive

darkzzx4avcsuofgfez5zq75cqc4mprjvfqywo-45dfcaxrwqg6qrlfid.onion


Darknetlive
Home
Arrests
Markets
Crypto
Forums
Onions
Shops
POLIZEI
Austrian Man Arrested for Alleged Amphetamine Purchase
Austrian police arrested a man for allegedly buying ecstasy and amphetamine on the darkweb.
Washington Man Admits Selling Fake Oxys on the Darkweb
A Washington man pleaded guilty to distributing a wide variety of drugs through the darkweb, including counterfeit oxycodone pills.
Dread V3: New Captcha, Market Standards, Search, and More
Dread is back online. The update, Dread V3, includes some of the most significant changes in Dread's history.

FlashLight Deep Web News

Another website about news from the Deep Web.



http://ovgl57qc3a5abwqgdhdtssvmydr6f6mjz6ey23thwy-63pmbxqmi45iid.onion/

The Intercept

Fearless, adversarial journalism that holds the powerful accountable.

https://27m3p2uv7igmj6kvd4ql3cct5h-3sdwrsajovkkndeufumzyfhlfev4qd.onion/

Dark Web Link

Dark Web Link is a promulgation (public announcement website) focused on providing the latest updates about the TOR browser, hidden DarkNet markets and all sorts of facts and information regarding the Dark Web sites, Deep Web sites, cybersecurity, cryptocurrencies, and tutorials. We strive to offer you upgraded reports, reviews, and fascinating Dark Web news that are most relevant in all aspects.

dwlonion3o3pjqsl.onion

https://darkweblink.com/

There are two primary writers on this site:
Cameron Cooke

https://darkweblink.com/author/cameron/

A passionate engineer and new technologies advocate, writing about new pieces of stuff is what Cameron Cooke writes about. He takes a deep interest in Dark Web and thus spends most of his time knowing and writing about the Dark Web Market, Deep Web Links and Websites.

Berjouhi Smith

https://darkweblink.com/author/berjouhi/

Berjouhi Smith is a staff writer for CBS Interactive covers topics on Dark Web for Dark Web Links. She has previously covered politics for CBSNews.com, as well as the intersection of technology and politics for CNET. Berjouhi has graduated with a B.A. in communication from Stanford University. She is highly influenced by various aspects of the Dark Web leading to be a writer for the Dark Web Link.

Chat Rooms

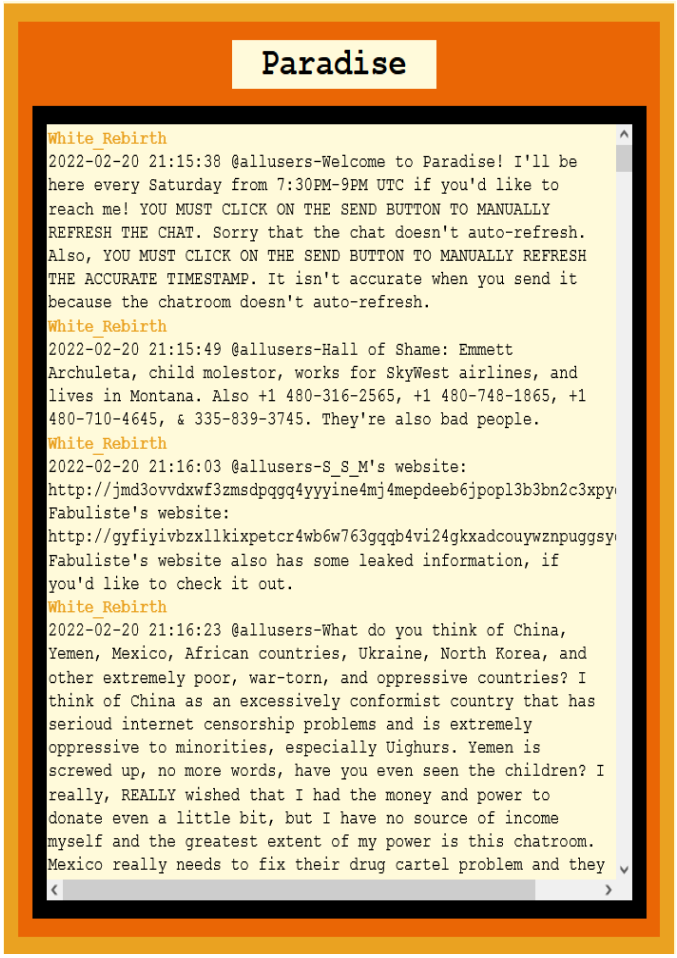
Hard to see anything of any real value here.

Paradise

http://4drjmo7z2dld4mci2limogypdibxxpg7dad6g-2snnrdufw6lcradc2qd.onion/

You are logged in! Welcome to Paradise!

Log Out


Paradise
White_Rebirth
2022-02-20 21:15:38 @allusers-Welcome to Paradise! I'll be here every Saturday from 7:30PM-9PM UTC if you'd like to reach me! YOU MUST CLICK ON THE SEND BUTTON TO MANUALLY REFRESH THE CHAT. Sorry that the chat doesn't auto-refresh. Also, YOU MUST CLICK ON THE SEND BUTTON TO MANUALLY REFRESH THE ACCURATE TIMESTAMP. It isn't accurate when you send it because the chatroom doesn't auto-refresh.
White_Rebirth
2022-02-20 21:15:49 @allusers-Hall of Shame: Emmett Archuleta, child molestor, works for SkyWest airlines, and lives in Montana. Also +1 480-316-2565, +1 480-748-1865, +1 480-710-4645, & 335-839-3745. They're also bad people.
White_Rebirth
2022-02-20 21:16:03 @allusers-S_S_M's website: http://jmd3ovvdxwf3zmsdpqgq4yyyine4mj4mepdeeb6jpopl3b3bn2c3xpy
Fabuliste's website: http://gyfiyivbzxllkixpetcr4wb6w763gqqb4vi24gkxadcouywznpuggsy
Fabuliste's website also has some leaked information, if you'd like to check it out.
White_Rebirth
2022-02-20 21:16:23 @allusers-What do you think of China, Yemen, Mexico, African countries, Ukraine, North Korea, and other extremely poor, war-torn, and oppressive countries? I think of China as an excessively conformist country that has serioud internet censorship problems and is extremely oppressive to minorities, especially Uighurs. Yemen is screwed up, no more words, have you even seen the children? I really, REALLY wished that I had the money and power to donate even a little bit, but I have no source of income myself and the greatest extent of my power is this chatroom. Mexico really needs to fix their drug cartel problem and they

Extremely primitive.

element

http://256ah7vgwpsh37bsz4jgcvepxy7ssnw3biql6a6gzrid-7haztnwsleid.onion/

Sorry, Element requires JavaScript to be enabled.

https://element.io/

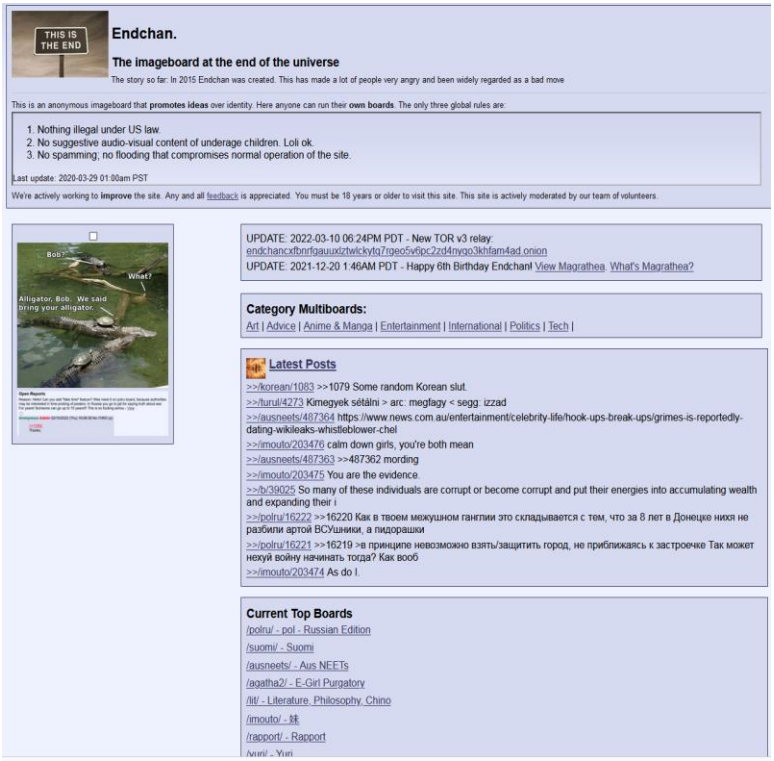
Secure and independent communication, connected via Matrix

Endchan

The image board at the end of the universe

The story so far: In 2015, Endchan was created. This has made a lot of people very angry and been widely regarded as a bad move.

http://enxx3byspwsdo446jujc52ucy2pf5urdbhqw3kbsfhlfjwmbpj-5smdad.onion/


Endchan.
The imageboard at the end of the universe
The story so far: In 2015 Endchan was created. This has made a lot of people very angry and been widely regarded as a bad move
This is an anonymous imageboard that promotes ideas over identity. Here anyone can run their own boards. The only three global rules are:
1. Nothing illegal under US law.
2. No suggestive audio-visual content of underage children. Loli ok.
3. No spamming; no flooding that compromises normal operation of the site.
Last update: 2020-03-29 01:00am PST
We're actively working to improve the site. Any and all feedback is appreciated. You must be 18 years or older to visit this site. This site is actively moderated by our team of volunteers.
Bob?
What?
Alligator, Bob. We said bring your alligator.
UPDATE: 2022-03-10 06:24PM PDT - New TOR v3 relay:
endchancxfbnrfgauuxlztwlckytq7rgeo5v6pc2zd4nvqo3khfam4ad.onion
UPDATE: 2021-12-20 1:46AM PDT - Happy 6th Birthday Endchan! View Magrathea. What's Magrathea?
Category Multiboards:
Art | Advice | Anime & Manga | Entertainment | International | Politics | Tech |
Latest Posts
>>/korean/1083 >>1079 Some random Korean slut.
>>/turul/4273 Kimegyek sétálni > arc: megfagy < segg: izzad
>>/ausneets/487364 https://www.news.com.au/entertainment/celebrity-life/hook-ups-break-ups/grimes-is-reportedly-dating-wikileaks-whistleblower-chel
>>/imouto/203476 calm down girls, you're both mean
>>/ausneets/487363 >>487362 mording
>>/imouto/203475 You are the evidence.
>>/b/39025 So many of these individuals are corrupt or become corrupt and put their energies into accumulating wealth and expanding their i
>>/polru/16222 >>16220 Как в твоем межушном ганглии это складывается с тем, что за 8 лет в Донецке ихня не разбили артой ВСУшники, а пидорашки
>>/polru/16221 >>16219 >в принципе невозможно взять/защитить город, не приближаясь к застроечке Так может нехуй войну начинать тогда? Как вооб
>>/imouto/203474 As do I.
Current Top Boards
/polru/ - pol - Russian Edition
/suomi/ - Suomi
/ausneets/ - Aus NEETs
/agatha2/ - E-Girl Purgatory
/lit/ - Literature, Philosophy, Chino
/imouto/ - 妹
/rapport/ - Rapport
/yuri/ - Yuri

2chan, 4chan, 8chan, oh my!

Exponential Hate

HATE those _who_ are different, or HATE _to be_ different?

Futaba Channel or Futaba for short, also sometimes called **2chan** (not to be confused with 2channel), is an imageboard in Japan. A popular Japanese website, it deals with a wide variety of topics, from daily personal problems to junk food, sports, ramen, and otaku and underground culture.

Origin

Futaba Channel was set up on August 30, 2001, as a refuge for 2channel users when 2channel was in danger of shutting down. It started as a textboard but eventually added imageboards based on the GazouBBS software. The English-language imageboard 4chan website was based on Futaba.

Concept

Futaba Channel consists of about 60 imageboards (three of which are oekaki boards) and about 40 textboards, with topics ranging from daily personal problems to junk food, sports, ramen, and pornography. There is also a place to upload general non-image files. Futaba is powered by a custom script based on GazouBBS (gazou.php. The Futaba script was open source (last updated in 2005) and its ancestors are used to run many Japanese and English imageboards.

Culture

Futaba has spawned a number of visual gags and characters; the OS-tans would be one such meme that has spread to western internet culture. Some of the characters that appear on Futaba Channel have entered the real world in the form of various real-life goods, such as figures, dolls or images printed on pillows. Such items are mainly produced by Japanese dōjin artists and groups.

Non-Japanese Internet users sometimes refer to Futaba Channel as 2chan, due to the address of the site. It is frequently unclear whether this is intended to mean Futaba Channel or 2channel, and sometimes it even refers to both, as if they were a single website. To eliminate confusion, the names Futaba and 2channel are often used.

https://en.wikipedia.org/wiki/Futaba_Channel

4chan is an anonymous English-language imageboard website. Launched by Christopher "moot" Poole in October 2003, the site hosts boards dedicated to a wide variety of topics, from anime and manga to video games, cooking, weapons, television, music, literature, history, fitness, politics, and sports, among others. Registration is not available and users typically post anonymously. As of 2022, 4chan receives more than 22 million unique monthly visitors, of which approximately half are from the United States.

4chan was created as an unofficial English-language counterpart to the Japanese imageboard Futaba Channel, also known as **2chan**, and its first boards were created for posting images and discussion related to anime. The site has been described as a hub of Internet subculture, with its community being influential in the formation of prominent Internet memes, such as lolcats, Rickrolling, rage comics, and Wojaks, as well as hacktivist and political movements, such as Anonymous and the alt-right. 4chan has often been the subject of media attention as a source of controversies, including the coordination of pranks and harassment against websites and Internet users, and the posting of illegal and offensive content. The Guardian summarized the 4chan community of 2008 as "lunatic, juvenile brilliant, ridiculous and alarming".

https://en.wikipedia.org/wiki/4chan

8kun, previously called **8chan**, Infinitechan or Infinitychan (stylized as ∞chan), is an imageboard website composed of user-created message boards. An owner moderates each board, with minimal interaction from site administration.[1] The site has been linked to white supremacism, neo-Nazism, the alt-right, racism and antisemitism, hate crimes, and multiple mass shootings. The site has been known to host child pornography; as a result, it was filtered out from Google Search in 2015. Several of the site's boards played an active role in the Gamergate controversy, encouraging Gamergate affiliates to frequent 8chan after 4chan banned the topic. 8chan is the home of the discredited far-right QAnon conspiracy theory.

Shortly before the 2019 El Paso shooting, a four-page message justifying the attack was posted to the site, and police have stated that they are "reasonably confident" it was posted by the perpetrator. In the aftermath of the back-to-back mass shootings on August 3 in El Paso and August 4 in Dayton, Ohio, respectively, the site was taken off Clearnet on August 5, 2019, when network infrastructure provider Cloudflare stopped providing their content delivery network (CDN) service. Voxility, a web services company that had been renting servers to Epik, the site's new domain registrar, as well as Epik's CDN provider subsidiary BitMitigate, also terminated service. After several attempts to return to Clearnet were ultimately stymied by providers denying service to 8chan, the site returned to the Clearnet as 8kun in November 2019 through a Russian hosting provider.

https://en.wikipedia.org/wiki/8chan

Does 4chan use Javascript, block Tor postings, and block VPNs? Are these not serious anonymity and privacy red flags?

8chan.moe

Welcome to 8chan.moe, the infinitely expanding imageboard!

http://4usoivrpy52lmc4mgn2h34cmfiltslesthr-56yttv2pxudd3dapqciyd.onion/

Welcome to 8chan.moe, the infinitely expanding imageboard!
On 8chan, you can create your own imageboard for free with no experience or programming knowledge needed.
Embrace the moe!
logs • archives • daily graphs • global rules • links • about • contact • donate • account
The backup domain is located at 8chan.se. .cc is a third fallback. TOR access can be found here, or you can access the TOR portal from the clearnet at Redchannit 2.0.
Please be aware of the Site Fallback Plan!
In case outages in Eastern Europe affect site availability, we will work to restore service as quickly as possible.
8chan.moe is a hobby project with no affiliation whatsoever to the administration of any other "8chan" site, past or present.
Stats
Total posts: 2574352
Posts in last hour: 251
Unique recent IPs: 600
Total boards: 285
Media files stored: 542555
Total media size: 664.74 GB
Top Boards
/v/ - Video Games /b/ - Random /hisrol/ - Hispa Rol /tkr/ - Tickling Refuge /vore1/ - Vore /abdl/ - Adult Baby - Diaper Lover
/co/ - Comics & Cartoons /delicious/ - Cake /404/ - Not Found /digi/ - Net Hangout /ss/ - Straight Shota
/choroy/ - La elite intelectual chilena /pol/ - Politically Incorrect /interracial/ - Interracial /zoo/ - Zoophilia /rule34/ - Rule34 /nido/ - Nido.org
/fast/ - Sonic the Hedgehog /sm/ - Shotacon

Video Chat

Jitsi

Jitsi is a collection of free and open-source multiplatform voice (VoIP), video conferencing and instant messaging applications for the web platform, Windows, Linux, MacOS, iOS and Android

Dark Web: Cybercriminals sell over 500,000 Zoom accounts

https://www.techrepublic.com/article/dark-web-cybercriminals-sell-half-a-million-zoom-accounts/

Social Media

The Jabber network

A free & decentralized social networking platform

Welcome to Jabber

https://joinjabber.org/

http://uideufistqhz44fhgtxdmt5k3drkrh-62gldd7tgmefixy3uu2dwqgjyd.onion

Welcome to the Jabber community. On this page, we'll help you find a server and a client to join the Jabber network and start chatting with your friends, without giving away all your data. Jabber is decentralized, just like email. This means you need to find a server, and from there you'll be able to chat with everyone else.

This may be confusing at first, but Jabber addresses (JIDs) look just like email addresses. So for example if you have the account emma.goldman on server jabber.fr, your address will be emma.goldman@jabber.fr. Chatrooms (also called MUCs) also have similar addresses, like

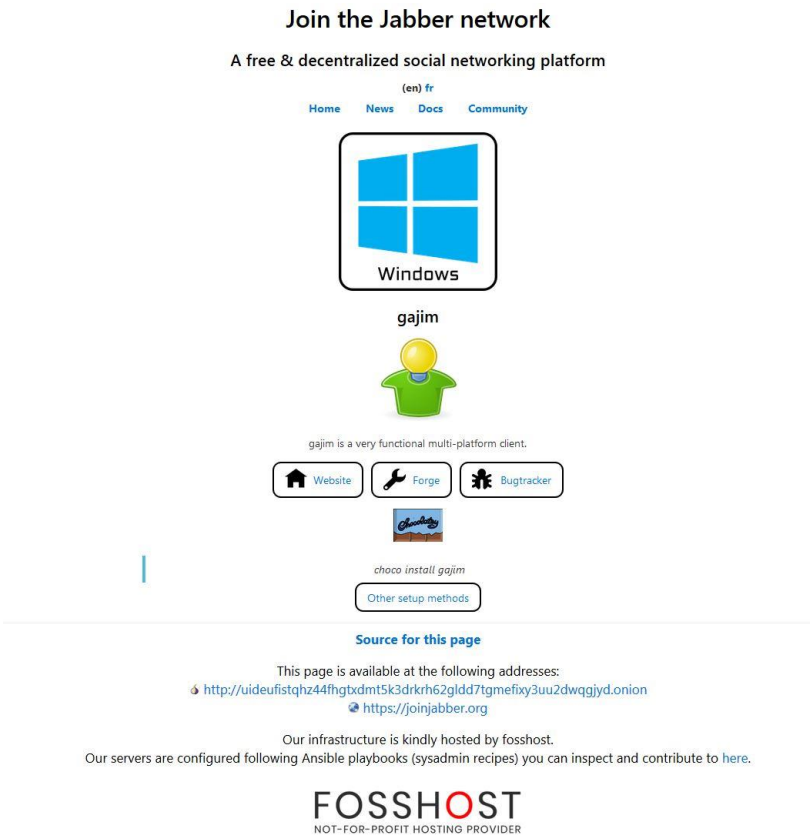
chat@joinjabber.org.

Jabber

Jabber.org is a public, free instant messaging (IM) and presence service, based on XMPP, an open standard for IM. (Instant Messaging)

Jabber.org was started in 1999 and has offered free instant messaging continuously since. It originally served as the development test bed for the jabberd project, the original Jabber/XMPP server. After becoming more stable it also became more popular with end users. As of 2012, it was a public production service, and one of the biggest nodes on the open XMPP network, with an average of 17,000 users logged in at a time.

https://en.wikipedia.org/wiki/Jabber



https://joinjabber.org/clients/windows/

https://xmpp.org/getting-started/

1. Download a client

There are many, many XMPP clients for you to choose from. To get you started, here are some of the more popular ones:

Desktop

- Beagle IM (macOS)
- Converse.js (Browser)
- Dino (Linux)
- Gajim (Linux, Windows)
- Monal (macOS)
- Swift.IM (Linux, macOS, Windows)
- UWPX (Windows)

I ran across this later, after I had already selected the suggested Gajim client.

Gajim

Gajim is an instant messaging client for the XMPP protocol which uses the GTK toolkit. The name Gajim is a recursive acronym for Gajim's a jabber instant messenger. Gajim runs on Linux, BSD, MacOS, and Microsoft Windows. Released under the GPL-3.0-only license, Gajim is free software. A 2009 round-up of similar software on Tom's Hardware found version 0.12.1 "the lightest and fastest jabber IM client". Wikipedia

Gtk Absolute Jabber Instant Messenger (Gajim)

The GTK library contains a set of graphical control elements (); version 3.22.16 contains 186 active and 36 deprecated widgets. GTK is an object-oriented widget toolkit written in the programming language C; it uses GObject, that is the GLib object system, for the object orientation. While GTK is mainly for windowing systems based on X11 and Wayland. GTK - Wikipedia

https://en.wikipedia.org/wiki/GTK

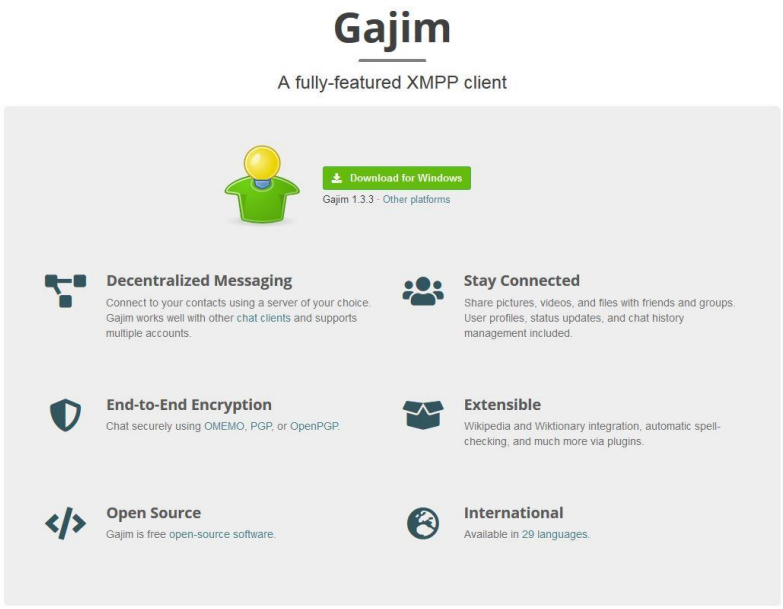
Extensible Messaging and Presence Protocol (XMPP) Wow, that is a mouthful.

Extensible Messaging and Presence Protocol (XMPP, originally named Jabber) is an open communication protocol designed for instant messaging (IM), presence information, and contact list maintenance. Based on XML (Extensible Markup Language), it enables the near-real-time exchange of structured data between two or more network entities.

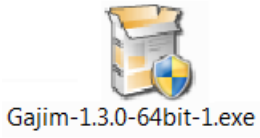
https://en.wikipedia.org/wiki/Xmpp

Public XMPP servers

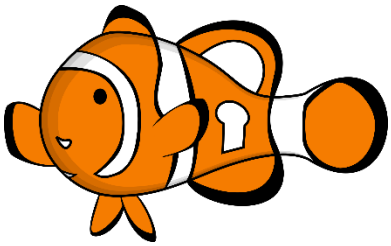
https://list.jabber.at/


Gajim
A fully-featured XMPP client
Download for Windows
Gajim 1.3.3 · Other platforms
Decentralized Messaging
Connect to your contacts using a server of your choice. Gajim works well with other chat clients and supports multiple accounts.
Stay Connected
Share pictures, videos, and files with friends and groups. User profiles, status updates, and chat history management included.
End-to-End Encryption
Chat securely using OMEMO, PGP, or OpenPGP.
Extensible
Wikipedia and Wiktionary integration, automatic spell-checking, and much more via plugins.
Open Source
Gajim is free open-source software.
International
Available in 29 languages.

gajim.org
Win10 1.3.3
https://gajim.org/downloads/
Win7 1.3.0 32 or 64 bit



From the FAQ:
Does Gajim support OMEMO encryption?
Yes, there is an OMEMO plugin.



Logo by fiaxh

https://github.com/siacs/Conversations/blob/master/art-/omemo_logo.svg, CC BY-SA 4.0,

https://commons.wikimedia.org/w/index.php?curid=46134840

OMEMO is an extension to the Extensible Messaging and Presence Protocol (XMPP) for multi-client end-to-end encryption developed by Andreas Straub. According to Straub, OMEMO uses the Double Ratchet Algorithm "to provide multi-end to multi-end encryption, allowing messages to be synchronized securely across multiple clients, even if some of them are offline".[1] The name "OMEMO" is a recursive acronym for "OMEMO Multi-End Message and Object Encryption". It is an open standard based on the Double Ratchet Algorithm and the Personal Eventing Protocol (PEP, XEP-0163).[2] OMEMO offers future and forward secrecy and deniability with message synchronization and offline delivery.

https://en.wikipedia.org/wiki/OMEMO

Based on my specific experience however, this function is already available without any additional efforts. But let us try this:

https://dev.gajim.org/gajim/gajimplugins//wikis/-OmemoGajimPlugin

So when you go there you get this:

Well, it turns out this this is a dead link. I suspect that the

OMEMO encryption is defunct or at least unsupported.

Shot off a test chat message in Gajim to a dread mod:

4/4/2022 | 3:12:28 PM n0stis: I am learning this Gajim, is my message encrypted?

Thanks, n0stis

4/4/2022 | 3:12:49 PM Cyberjagu: ?OTRv23? Cyberjagu@jabber.calyxinstitute.org/ has requested an Off-the-Record private conversation. However, you do not have a plugin to support that. See https://otr.cypherpunks.ca/ for more information.

4/4/2022 | 3:15:09 PM No devices found. Query in progress...

https://otr.cypherpunks.ca/ pidgin-otr-4.0.2.exe

So let us now blow off all my work with Gajim and let us start anew with Off-the-Record which is apparently an encrypted chat protocol supported in a some chat software programs including one called Pidgin.

Chat

Pidgin, and Off the Record (OTR)

Off-the-Record Messaging (OTR) is a cryptographic protocol that provides encryption for instant messaging conversations. OTR uses a combination of AES symmetric-key algorithm with 128 bits key length, the Diffie–Hellman key exchange with 1536 bits group size, and the SHA-1 hash function. In addition to authentication and encryption, OTR provides forward secrecy and malleable encryption.

https://en.wikipedia.org/wiki/Off-the-Record_Messaging

Pidgin (formerly named Gaim) is a free and open-source multi-platform instant messaging client, that has support for many instant messaging protocols, allowing the user to simultaneously log in to various services from a single application. Pidgin is widely used for its Off-the-Record Messaging (OTR) plugin, which offers end-to-end encryption

https://en.wikipedia.org/wiki/Pidgin_(software)

Dark Web Monitoring

How to monitor the Dark Web

As the early signs of cyber-attacks can be traced back to anonymous communications in the Deep Web, a complete risk prevention system has to deal systematically with any type of content related to the brand in question.

A global cyber surveillance and monitoring platform like Massive's Strixus allows companies of any size to enjoy complete security and protection, because any type of suspicious activity can be detected immediately. Strixus early warning system means that the correct strategies can be put into place to fight any type of threat. The Deep Web is carefully monitored 24/7 to make sure that your company is 100% safe.

https://www.massivealliance.com/blog/2013/10/23/deep-web/

DNstats

Documenting the day-to-day happenings of the DarkNet

https://dnstats.net/

Surveilled

(abused and exploited)

Surveillance [ser-vey-luh ns, -veyl-yuh ns] noun

- a watch kept over a person, group, etc., especially over a suspect, prisoner, or the like
- continuous observation of a place, person, group, or ongoing activity to gather information
- attentive observation, as to oversee and direct someone or something

Surveillance is the monitoring of behavior, activities, or information for the purpose of influencing, managing or directing. This can include observation from a distance by means of electronic equipment, such as closed-circuit television, or interception of electronically transmitted information, such as Internet traffic. It can also include simple technical methods, such as human intelligence gathering and postal interception.

https://en.wikipedia.org/wiki/Surveillance

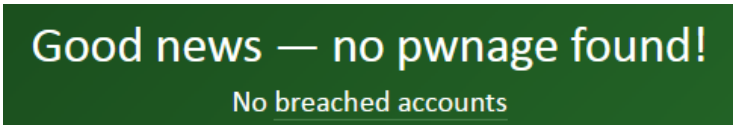
https://ssd.eff.org/en/module-categories/basics

The easiest way to Stop this from happening is to STOP using all personal, car, and home surveillance devices!

A neat guide on "Assessing Your Risks" from the Electronic Frontier Foundation:

https://ssd.eff.org/en/module/assessing-your-risks

Check your email account and phone numbers to see if they have been compromised.



https://haveibeenpwned.com/

ShieldsUp

https://www.grc.com/shieldsup

ShieldsUp is an online port scanning service created by Steve Gibson of Gibson Research Corporation and hosted at grc.com. The purpose of this utility is to alert the users of any ports that have been opened through their firewalls or through their NAT routers. The utility can scan the most common file sharing ports, as well as all service ports, and user defined ports, in sets of 64.

After you check your router, check your File Sharing and Common Ports.

What's DNS poisoning, anyway?

DNS poisoning and its DNS cache-poisoning relative allow hackers to replace the legitimate DNS lookup for a site such as google.com or arstechnica.com—normally 209.148.113.38 and 18.117.54.175, respectively—with malicious IP addresses that can masquerade as those sites as they attempt to install malware, phish passwords, or carry out other nefarious actions.

https://arstechnica.com/information-technology/2022/05/gear-from-netgear-linksys-and-200-others-has-unpatched-dns-poisoning-flaw/

Here are a few news stories for you to think about:

Google is disabling Xiaomi integrations on our devices' after a Nest Hub user picked up random pics from strangers' feeds

"Among the eight examples initially provided are a handful of disturbingly clear images showing a sleeping baby, a security camera's view of an enclosed porch, and a man seemingly asleep in a chair." A camera owner reported receiving still images from other random peoples' homes when he tried to stream content from his camera to a Google Nest Hub.

Android Police broke the story, and published some photos that are horrifying, privacy-wise, if legit. androidpolice.com *(Android Police is an American technology news and a blog dedicated to everything related to Android smartphones.)*

Google responded:

"We're aware of the issue and are in contact with Xiaomi to work on a fix. In the meantime, we're disabling Xiaomi integrations on our devices."

2019 was the year of voice assistant privacy dumpster fires

2019 was the "I Told You So" year for privacy advocates and voice assistants: the year in which every company that wanted you to trust them to put an always-on microphone in the most intimate places in your home. They were revealed to have allowed thousands of low-waged contractors to listen in on millions of clips, many of them accidentally recorded. First, it was Amazon, then Google, then Apple, then Microsoft.

What's more and worse, is that these arms-length contractors who were getting your stolen audio were working under terrible conditions, in sweatshops where they were worked long hours, listening to potentially traumatizing audio Voice assistants have proven to be no more secure than any of Big Tech's other products.

The true believers in voice computing started to build voice assistants in full knowledge that these will not only be perceived as creepy, but that they will be creepy. These companies lie to their customers, and even to Congress, about whether this is going on.

A former data analyst who worked on Apple Siri transcriptions for several years says workers swapped horror stories during smoke breaks. A current analyst, asked to recount the most outrageous clip to come through, says it was something akin to a scene from Fifty Shades of Grey.

https://boingboing.net/2019/12/12/not-ok-google.html

Silicon Valley Is Listening to Your Most Intimate Moments

How the world's biggest companies got millions of people to let temporary workers analyze some very sensitive recordings.

She could not believe what she was hearing. She had been hired by a temporary agency for a vague job: transcribing audio files for Amazon.com Inc. For $12 an hour, she and her fellow contractors, or "data associates," listened to snippets of random conversations and jotted down every word on their laptops. The clips included recordings of intimate moments inside people's homes.

https://www.bloomberg.com/news/features/2019-12-11/silicon-valley-got-millions-to-let-siri-and-alexa-listen-in

Amazon Workers Are Listening to What You Tell Alexa

A global team reviews audio clips in an effort to help the voice-activated assistant respond to commands. Tens of millions of people use smart speakers and their voice software to play games find music or trawl for trivia. Millions more are reluctant to invite the devices and their powerful microphones into their homes out of concern that someone might be listening.

Sometimes, someone is.

https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio

Microsoft's Cortana is sleeping with the fishes

Many people are fine with allowing a helpful wiretap into their lives. I am not one of them. None of them. When I heard that Cortana was being sent out to pasture by Microsoft, I was excited. The dismantling of surveillance apparatus that has slimed its way into our daily lives always leaves me feeling a little frisky.

Despite dropping the app in some regions, Cortana itself remains "an integral part" of the company's business model to incorporate "conversational computing and productivity" into its products according to the spokesperson, so Microsoft does not appear to be closing the coffin on it entirely. Last year, Microsoft's CEO admitted that the company's virtual assistant could not keep up with the likes of Alexa or Siri.

https://boingboing.net/2019/11/18/microsofts-cortana-is-sleep.html

The Chilling Side Effects of Mass Surveillance

Nothing to Hide?

"He who does not move, does not notice his chains" – Rosa Luxemburg

The definition of "bad" may mean one thing to those who are "good," but the people in power have the last say in what "bad" means. Bad could be anything that impedes the government's ability to pursue its interests, or exercise its power.

Mark Zuckerberg, CEO and founder of Facebook, says privacy is no longer a social norm, yet he has used his millions to create his own personal privacy by buying all the properties around his house.

Surveillance impedes creativity and freedom of expression. People alter their behaviors to conform when they know that they can be watched at any time. Just like when you were a child under your parents watchful eyes.

A panopticon is a type of architectural design devised by an 18th Century English philosopher and social theorist. The concept is to allow a single person to observe all the members of a group or class. It was devised for prisons, but is also used in computer labs in schools, school buses. Since it is physically impossible for one person to observe all subjects at once, obedience is obtained by the threat that anyone can be watched at any time. The key to the design is that one person can watch any inmate, but the inmate cannot see the person, so you never know when you might be under surveillance.

A society in which people can be monitored at all times is a society that breeds conformity, obedience and submission, and why every tyrant likes this.

It is important however in a free and democratic society, to have the whistleblowers, journalists, and other activists who can to provide a balance to those who are in power. Mass surveillance severely curtails this ability.

The measure of how free a society is, is not how it treats its good, obedient, compliant citizens, but how it treats its whistleblowers, journalists, activists, dissidents, criminals, as well as its poor and disenfranchised.

The US and its partners, unknown to the entire world until the Snowden file leaks, has converted the Internet, once heralded as an unprecedented tool of liberation and democratization, into an unprecedented tool of mass, indiscriminate predatory corporate capitalist surveillance. The totalitarian state that George Orwell foretold of in his book 1984, and it has stripped us of our personal privacy and freedoms.

There are many issues that face our future generations, but the erosion of our personal privacy, freedoms, and liberties is a clear and present danger. 250 years ago, people fought those who opposed the ideals of life, liberty, and pursuit of happiness. Those principles are the foundation that allowed the rise of the United States of America. Now, that very foundation is being eroded using the half-cocked excuse of keeping us safe.

https://www.aljazeera.com/opinions/2013/6/25/the-chilling-effects-of-surveillance/

https://www.techdirt.com/2016/05/02/chilling-effect-mass-surveillance-quantified/

NSA Utah data center

Apple data center

Microsoft data center

Facebook data center

Google data center

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say." Ed Snowden

Also, see the Delete Facebook and Stop using Google and other essays in the appendices.

https://greggborodaty.com/chilling-side-effects-mass-surveillance/

https://www.ted.com/talks/glenn_greenwald_why_privacy_matters

Why collect it all?

The NSA and law enforcement want to use it against you, and change your thinking and actions.

The corporations want to use it to make money and change your thinking and behaviors.

Be aware that the example companies listed above have many, many, data centers like this around this country and in countries all over the world.

American Phone-Tracking Firm Demo'd Surveillance Powers by Spying on CIA and NSA

Anomaly Six, a secretive government contractor, claims to monitor the movements of billions of phones around the world and unmask spies with the press of a button.

https://theintercept.com/2022/04/22/anomaly-six-phone-tracking-zignal-surveillance-cia-nsa/

Other Resources

- https://www.whatsmybrowser.org/
- https://www.privacytools.io/
- https://restoreprivacy.com/

Honeynet Project

The Honeynet Project is a leading international 501c3 non-profit security research organization, dedicated to investigating the latest attacks and developing open source security tools to improve Internet security. With Chapters around the world, our volunteers have contributed to fight against malware (such as Confickr), discovering new attacks and creating security tools used by businesses and government agencies all over the world. The organization continues to be on the cutting edge of security research by working to analyze the latest attacks and educating the public about threats to information systems across the world.

- *https://www.honeynet.org/*

Data Brokers

China's Great Firewall, the UK's Snooper's Charter, the US' mass surveillance and bulk data collection -- compliments of the National Security Agency (NSA) and Edward Snowden's whistleblowing -- Russia's insidious election meddling, and countless censorship and communication blackout schemes across the Middle East are all contributing to a global surveillance state in which privacy is a luxury of the few and not a right of the many.

As surveillance becomes a common factor of our daily lives, privacy is in danger of no longer being considered an intrinsic right -- and it seems we, too, are adopting our own personal forms of online digital stalking and spying.

Digital bread crumbs, cookies (not a necessarily bad thing) to remember you but have now evolved to third party cookies that track you wherever you go, location, IP address, device, screen size. This is a bad thing.

Data brokers like Epsilon sell this info to anyone who will buy it.

Why is this a problem?

Your personal info not protected by HIPPA. The 4th Amendment does not protect you here.

The United States has no data privacy regulations like the European Charter of Fundamental Rights and The European Union’s General Data Protection Regulation (GDPR).

Marketing Company Agrees to Pay $150 Million for Facilitating 30 million Elder Fraud Schemes

https://www.justice.gov/opa/pr/marketing-company-agrees-pay-150-million-facilitating-elder-fraud-schemes

Epsilon solutions are built to solve your biggest challenges

To market effectively, brands need a clear view of their customers. Only Epsilon has the industry's most accurate, stable and scalable identity that's anchored in first-party data—not third-party cookies or device IDs that break down over time. And with award-winning, best-in-class digital media, messaging and loyalty solutions, brands deliver personalized messages at scale that grow real customer relationships. See why we're the only partner that can drive your marketing's success.

https://www.epsilon.com/us/about-us/who-we-are

Seems to be a bit of a conflict with:

Epsilon Data Management LLC

Epsilon is a full-service information technology partner, offering services ranging from compliance and cybersecurity to cloud management and call center support.

What can you do about it?

User software like Adaware (blocks advertising on websites)

https://www.adaware.com/

Use web browser extensions with anti-trackers like:

1. Duckduckgo Privacy Essentials (blocks tracking)
2. Ghostery (blocks trackers)
3. HTTPS Everywhere from the EFF (Electronic Frontier Foundation software that forces https secure encrypted connections), if not using Firefox or another browser with Enable **HTTPS-Only Mode in all windows** turned on.
4. Privacy Badger (EFF software to block trackers) I do not use this since Firefox supports https only.
5. JavaScript Restrictor (prevents malicious webpage scripts from running on your computer)

Go to your browser setting and **Manage Your Extensions (addons)** to add these to protect you.

Do not sign up for any tracking services or any software (apps) that may (most likely) track you.

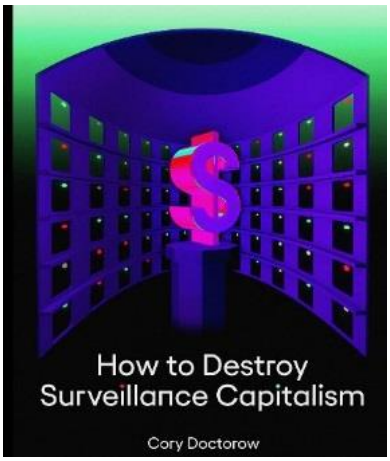
https://ssd.eff.org/en/module-categories/basics

Get a Free Dark Web Scan

While there's no way to ensure all your information stays private, putting protective measures in place can help. Knowing if and when your information is compromised can also help you respond quickly—before too much damage is done. Experian offers a free, one-time Dark Web scan for your Social Security number, email and phone number. If you want ongoing Dark Web surveillance, it's one of the many benefits included with an Experian IdentityWorksSM subscription.

Do you really want to give these data brokers your info if they don't already have it and are currently selling it?

For more on this subject, check out:



Doctorow, Cory. How to Destroy Surveillance Capitalism.

Documents obtained by a coalition of immigrant rights groups reveal ICE has contracted with the third-party data broker LexisNexis, allowing it to receive real-time jail booking data from sheriff's offices in the state of Colorado. The move to track the whereabouts of immigrants curtails Colorado's sanctuary policies, which are meant to prevent state and local law enforcement from cooperating with ICE. Jacinta González of Mijente's #NoTechForICE campaign said, "ICE agents once relied on the police to help them track us, arrest us, and deport us. Now, tech companies, by selling our personal data, are helping them instead."

https://www.democracynow.org/2022/4/22/headlines/private_data_brokers_help_ice_skirt_sanctuary_policies_and_target_immigrants

Data Breaches

A data breach is an incident where the secure storage of information was compromised. It could include accessing the information without authorization or knowledge of the data source. Data breaches hurt regular people by leaking and exposing their personal records and identity details but can also result in financial loss from identity theft and associated scams and unauthorized activity. Protect yourself with knowledge of what happened and what was breached by running one of our free data breach scans.

https://www.idstrong.com/data-breaches/

It seems that the supposed government white hat hackers cannot protect their tools from the black hats.

Vault 7 is a series of documents that WikiLeaks began to publish on 7 March 2017, detailing the activities and capabilities of the United States Central Intelligence Agency to perform electronic surveillance and cyber warfare. The files, dating from 2013 to 2016, include details on the agency's software capabilities, such as the ability to compromise cars, smart TVs, web browsers (including Google Chrome, Microsoft Edge, Mozilla Firefox, and Opera), and the operating systems of most smartphones (including Apple's iOS and Google's Android), as well as other operating systems such as Microsoft Windows, MacOS, and Linux. A CIA internal audit identified 91 malware tools out of more than 500 tools in use in 2016 being compromised by the release.

https://en.wikipedia.org/wiki/Vault_7

Data Breaches

Global Accounting Firm Deloitte Hit by Cyber Attack That Impacted Some Client's Confidential Data

Cyber-attacks are becoming more common than ever before. Although, this is not really that surprising, being that we now employ more cyber technologies within our daily operations than ever. Of course, these cyber implements can be valuable targets for attackers. There are certain industries that tend to be much more frequently targeted by malicious attackers due to the wide range of valuable data that they hold. This includes healthcare and governmental organizations, and of course, financial organizations. The reason that attackers heavily target the latter is quite obvious, being that they store massive amounts of financial data that can be used by attackers to achieve illicit gains. In a recent attack on a financial organization, the global accounting firm Deloitte was hit by a cyber-attack that resulted in a breach of some of its larger client's confidential data and plans.

https://www.massivealliance.com/blog/2017/09/28/global-accounting-firm-deloitte-hit-by-cyber-attack-that-impacted-some-clients-confidential-data/

Who Was Involved In The NSA Hack?

Harold T. Martin III, Nghia Pho, and a hacker group called the shadow brokers are all suspected of being involved in NSA's data breach.

Harold T. Martin III was found guilty of insider data breach and stealing piles of **50 terabytes** of confidential documents and computer information compiling the most significant data breach of the NSA ever. Although there is no evidence Mr. Martin (an ex contractor for the NSA's Tailored Access Operations hacking unit) sold or shared the information, The NSA data breach was not a single incident but three linked events. In Mr. Martin's case, the NSA discovered that he had been stealing information for more than 20 years from the NSA and other security agencies where he worked.it was leaked.

The National Security Agency (NSA) was the main attraction in a major data breach involving three different participants, and as a result, they had to change national security protocols and operations. The NSA is responsible for national security; therefore, it would seem that their systems and security measures would be impenetrable; not true.

The Shadow Brokers (TSB) is a hacker group who first appeared in the summer of 2016. They published several leaks containing hacking tools, including several zero-day exploits,[1] from the "Equation Group" who are widely suspected to be a branch of the National Security Agency (NSA) of the United States. Specifically, these exploits and vulnerabilities targeted enterprise firewalls, antivirus software, and Microsoft products. The Shadow Brokers originally attributed the leaks to the Equation Group threat actor, who have been tied to the NSA's Tailored Access Operations unit.

https://en.wikipedia.org/wiki/The_Shadow_Brokers

The Leaked NSA Spy Tool That Hacked the World

https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/

NSA Tools

Tools that make you look like a master hacker to your friends.

A few tools that will make you look like a master hacker to your friends who have no or little knowledge of programming/hacking.

None of these files are harmful and will do nothing special. They're just made for the show. https://sourceforge.net/projects/nsa-tools/

Ransomware

Ransomware is malware (malicious software) planted unknowingly in a computer or mobile device that disables its operation or access to its data, until the owner pays to regain control or access.

https://www.dictionary.com/browse/ransomware?s=t

Ransomware attacks are typically carried out using a Trojan that is disguised as a legitimate file, that the user is tricked (see Phishing) into downloading or opening when it arrives as an email attachment.

https://en.wikipedia.org/wiki/Ransomware

Organizations in the throes of cleaning up after a ransomware outbreak typically will change passwords for all user accounts that have access to any email systems, servers, and desktop workstations within their network. But all too often, ransomware victims fail to grasp that the crooks behind these attacks can and frequently do siphon every single password stored on each infected endpoint. The result of this oversight may offer attackers a way back into the affected organization, access to financial and healthcare accounts, or — worse yet — key tools for attacking **the victim's various business partners and clients**.

The point here is you could be infected by or have your login credentials stolen by one of your vendors or customers that have been attacked. For example:

-Identity and password management platforms Auth0 and LastPass
-Multiple personal and business banking portals;
-Microsoft Office365 accounts
-Direct deposit and Medicaid billing portals
-Cloud-based health insurance management portals
-Numerous online payment-processing services
-Cloud-based payroll management services
-Prescription management services
-Commercial phone, Internet and power services
-Medical supply services
-State and local government competitive bidding portals
-Online content distribution networks
-Shipping and postage accounts
-Amazon, Facebook, LinkedIn, Microsoft, Twitter accounts

In mid-November 2019, Wisconsin-based Virtual Care Provider Inc. (VCPI) was hit by the Ryuk ransomware strain. VCPI manages the IT systems for some 110 clients that serve approximately 2,400 nursing homes in 45 U.S. states. VCPI declined to pay the multi-million dollar ransom demanded by their extortionists, and the attack cut off many of those elder care facilities from their patient records, email and telephone service for days or weeks while VCPI rebuilt its network.

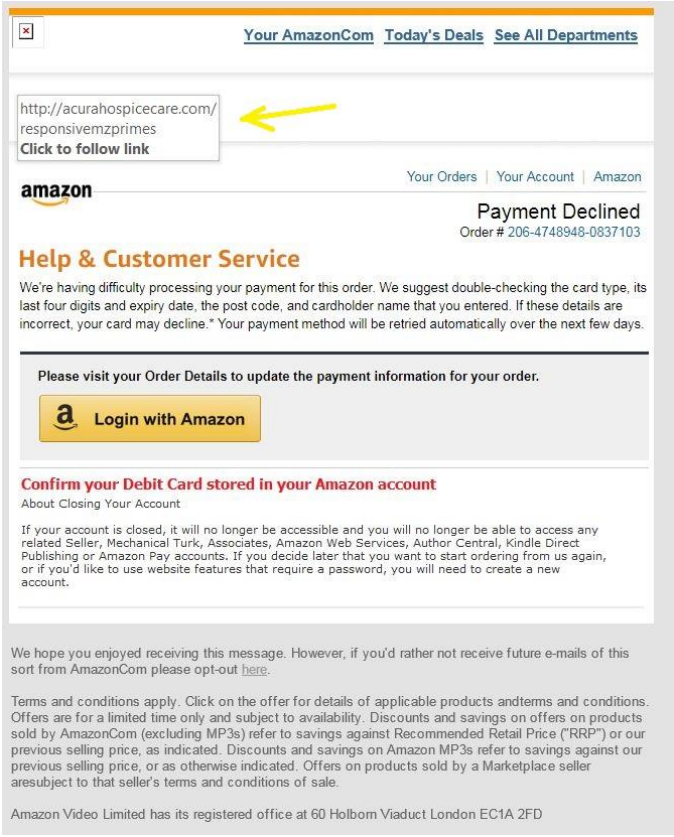
https://krebsonsecurity.com/

Many times, computer backup files which normally would be used to restore the systems are also effected, meaning encrypted, unless they are disconnected from the individual computers, the computer network, or stored off-site at the time of the attack.

There are many variants of Ransomware including WannaCry, Petya, NotPetya, and Jigsaw. These attacks include a message demanding payment by a date certain, usually in the form of untraceable Bitcoin cryptocurrency. Upon paying, the victim will receive an encryption key to unlock their files. Recently, many businesses, cloud-computing providers, and municipalities are not paying the ransom and suffering the consequences. To deter this, these bandits are now threating to make public all of the information stolen including documents, emails, and passwords.

If you are a company, hire a vendor like knowbe4.com to train your employees. They will also send out test spam messages and keep track of who the "clickers" are. They will lather, rinse, and repeat, until all the "clickers" are retrained.

If you are an individual, be suspicious of everything. If someone sends you a hyperlink or a button to click on in an email, hover your mouse cursor over it to see where it is going to direct you. If it is not a site you know, do not click! See example below:


Your AmazonCom Today's Deals See All Departments
http://acurahospicecare.com/responsivemzprimes
Click to follow link
Your Orders | Your Account | Amazon
amazon
Payment Declined
Order # 206-4748948-0837103
Help & Customer Service
We're having difficulty processing your payment for this order. We suggest double-checking the card type, its last four digits and expiry date, the post code, and cardholder name that you entered. If these details are incorrect, your card may decline.* Your payment method will be retried automatically over the next few days.
Please visit your Order Details to update the payment information for your order.
Login with Amazon
Confirm your Debit Card stored in your Amazon account
About Closing Your Account
If your account is closed, it will no longer be accessible and you will no longer be able to access any related Seller, Mechanical Turk, Associates, Amazon Web Services, Author Central, Kindle Direct Publishing or Amazon Pay accounts. If you decide later that you want to start ordering from us again, or if you'd like to use website features that require a password, you will need to create a new account.
We hope you enjoyed receiving this message. However, if you'd rather not receive future e-mails of this sort from AmazonCom please opt-out here.
Terms and conditions apply. Click on the offer for details of applicable products andterms and conditions. Offers are for a limited time only and subject to availability. Discounts and savings on offers on products sold by AmazonCom (excluding MP3s) refer to savings against Recommended Retail Price ("RRP") or our previous selling price, as indicated. Discounts and savings on Amazon MP3s refer to savings against our previous selling price, or as otherwise indicated. Offers on products sold by a Marketplace seller aresubject to that seller's terms and conditions of sale.
Amazon Video Limited has its registered office at 60 Holborn Viaduct London EC1A 2FD

Notice that this "follow the link" message indicated by the arrow is also not a secure encrypted https: address, but a clear text http: address. This is not normal nor acceptable for a payment related service.

How can you defend against ransomware?

1. Update your software. Use anti-virus software and keep it up-to-date. And set your operating system, web browser, and security software to update automatically on your computer. On mobile devices, you may have to do it manually. If your software is out-of-date, it is easier for criminals to sneak bad stuff onto your device.
2. Think twice before clicking on links or downloading attachments and apps. According to one panelist, 91% of ransomware is downloaded through phishing emails. You also can get ransomware from visiting a compromised site or through malicious online ads.
3. Back up your important files. From tax forms to family photos, make it part of your routine to back up files on your

computers and mobile devices often. When you are done, log out of the cloud and unplug external hard drives so hackers cannot encrypt and lock your back-ups, too.

What if you are a victim of ransomware?

1. Contain the attack. Disconnect infected devices from your network to keep ransomware from spreading.
2. Restore your computer. If you have backed up your files, and removed any malware, you may be able to restore your computer. Follow the instructions from your operating system to re-boot your computer, if possible.
3. Contact law enforcement. Report ransomware attacks to the Internet Crime Complaint Center or an FBI field office. Include any contact information (like the criminals' email address) or payment information (like a Bitcoin wallet number). This may help with investigations.

Should you pay the ransom?

Law enforcement does not recommend paying the ransom, although it is up to you to determine whether the risks and costs of paying are worth the possibility of getting your files back. If you pay the ransom, there is no guarantee you will get your files back. In fact, agreeing to pay signals to criminals that you have not backed up your files. Knowing this, they may increase the ransom price — and may delete or deny access to your files anyway. Even if you do get your files back, they may be corrupted. And you might be a target for other scams.

https://www.consumer.ftc.gov/blog/2016/11/how-defend-against-ransomware

How to Recognize and Avoid Phishing Scams

Scammers use email or text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like these every day — and they are often successful. The FBI's Internet Crime Complaint Center reported that people lost $30 million to phishing schemes in one year. But there are several things you can do to protect yourself.

https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

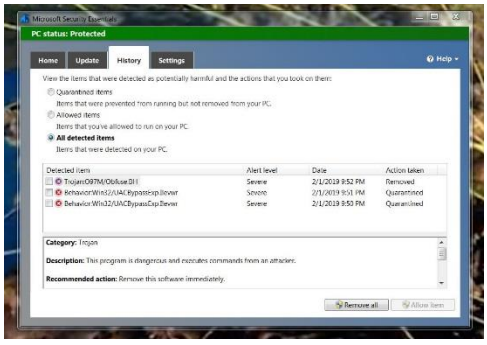
Pay some attention to what you are doing online and you will be fine.

Malware

Malware (a portmanteau for malicious software) is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive users access to information or which unknowingly interferes with the user's computer security and privacy.

Many types of malware exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wiper, and scareware. The defense strategies against malware differs according to the type of malware but most can be thwarted by installing antivirus software, firewalls, applying regular patches to reduce zero-day attacks, securing networks from intrusion, having regular backups and isolating infected systems.

https://en.wikipedia.org/wiki/Malware



Microsoft Security Essentials

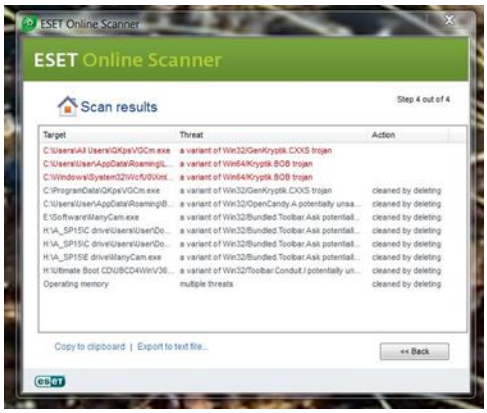
Microsoft Security Essentials (MSE) is an antivirus software (AV) product that provides protection against different types of malicious software, such as computer viruses, spyware, rootkits, and Trojan horses. Prior to version 4.5, MSE ran on Windows XP, Windows Vista, and Windows 7, but not on Windows 8 and later versions, which have built-in AV components known as Windows Defender. MSE 4.5 and later versions do not run on Windows XP. The license agreement allows home users and small businesses to install and use the product free-of-charge.

Microsoft Security Essentials automatically checks and downloads the latest virus definitions from Microsoft Update which is updated three times a day.

Note: MS has greatly improved this technology from what was originally labeled by users as their DCS technology. (Doesn't Catch Shit)

ESET

Blocks ransomware attacks and hackers
Enables you to shop and bank online securely
Protects your Windows, macOS and Android devices
Encrypts your files and safely stores your passwords
Easy installation and setup - set and forget!
Personalized protection against never-before-seen threats
Manage and monitor the security of your Windows and Android home devices on the go



https://www.eset.com/int/home/online-scanner/

Malwarebytes Anti-Malware

Malwarebytes Anti-Malware is an anti-malware software for Microsoft Windows, MacOS and Android OS that finds and removes malware.

https://www.malwarebytes.com

Managing attachments with Dangerzone

Have you ever heard the computer security advice, “Don’t open attachments”? This is solid advice, but unfortunately for journalists, activists, and many other people, it’s impossible to follow. Imagine if you were a journalist and got an email from someone claiming to work for the Trump Organization with “Donald Trump tax returns.pdf” attached. Are you really going to reply saying, “Sorry, I don’t open attachments” and leave it at that?

Dangerzone aims to solve this problem. You can install Dangerzone on your Mac, Windows, or Linux computer, and then use it to open a variety of types of documents: PDFs, Microsoft Office or LibreOffice documents, or images. Even if the original document is dangerous and would normally hack your computer, Dangerzone will convert it into a safe PDF that you can open and read.

You can think of it like printing a document and then rescanning it to remove anything sketchy, except all done in software.

Download Dangerzone for Windows, MacOS, or Linux to get started.

URL defanging

We all know that plain text emails are not as effective at catching attention, not as easy to read, and not as well received when communicating with non-technical users as are rich text. (html).

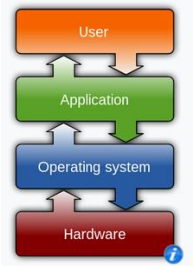
URL defanging is the standard term for making URLs non-clickable (e.g. using hxxps:// vs https://).

Email remains the primary source of compromised accounts (phishing, malware and ransomware) either through malicious attachments or clickable malicious URLs. Anti-virus/anti-malware solutions do an effective job of automatically protecting us from malicious attachments, but are not able to protect us from malicious URLs.

Defanging a URL ensures that users must make a deliberate decision to visit the intended destination by copying and pasting the URL into their browser address bar. This is intended to raise the security awareness of end users, which in turn decreases the likelihood of successful phishing attempts.

Operating Systems

An operating system (OS) is system software that manages computer hardware, software resources, and provides common services for computer programs. https://en.wikipedia.org/wiki/Operating_system



Tails/Whonix/Qubes

Note: If you are sufficiently experienced and motivated, feel free to ignore most of this advice. Much like highway speed limit signs, they can be looked on as suggestions mostly for visiting tourists.

Using a secure operating system is one of the most important parts of using the DarkNet.

Tails

If you are a new user or someone not very tech savvy you should stick with using tails. Why tails? Tails is secure live operating system that will work out of the box. Most software you need will be included in Tails.

Whonix/Qubes

Using a Whonix/Qubes setup is one of the most secure setups. The setup is very advanced; if you do not configure everything correctly, you can potentially hurt your OpSec[16] or put yourself at risk. If you do not know what you are doing just stick with using Tails.

[16] *Operational Security*

Whonix:

An alternative to Tails and also an open source project. Whonix is an operating system focused on anonymity, privacy, and security. It's based on the Tor anonymity network, Debian GNU/Linux, and security by isolation. DNS leaks are impossible and not even malware with root privileges can find out the user's real I.P. address. Official Site: https://www.whonix.org/

Whonix For The Darknet Markets:

http://archivecaslytosk.onion/COfTH

https://en.wikipedia.org/wiki/Whonix

https://www.whonix.org/wiki/Documentation

Whonix Documentation concerning Data Collection techniques

https://www.whonix.org/wiki/Data_Collection_Techniques

https://www.whonix.org/wiki/Warning

https://www.whonix.org/wiki/Dev/Threat_Model

https://www.whonix.org/wiki/Comparison_with_Others[Archive.org

Qubes:

Qubes OS is a security-focused desktop operating system that aims to provide security through isolation. Virtualization is performed by Xen, and user environments can be based on Fedora, Debian, Whonix, and Microsoft Windows, among other operating systems.

Qubes implements a Security by Isolation approach. The assumption is that there can be no perfect, bug-free desktop environment: such an environment counts millions of lines of code and billions of software/hardware interactions. One critical bug in any of these interactions may be enough for malicious software to take control over a machine.

To secure a desktop a Qubes user takes care to isolate various environments, so that if one of the components gets compromised, the malicious software would get access to only the data inside that environment.

https://en.wikipedia.org/wiki/Qubes_OS

Some DW users, perhaps most, would say that running the Whonix OS in a Qubes VM is the most secure (privacy and anonymity) system that is available by a long way.

Others, perhaps not raised from pup to adult by a pack of wild free range Whonix users, would say that comfortable proficiency in this type of system requires the equivalent effort of obtaining an undergraduate degree. This in fact requires years not months of study and practice. They would question the intentions, motivations, and perhaps sanity, of anyone who would to exert this amount of time and energy to learn and use a single computer operating system.

The following message thread from the dread DW OpSec forum perhaps best illustrates each of these points of view.

Things to keep in mind while using Whonix in QubesOS.

by /u/decaptchamyass in /d/OpSec

We all are pretty much aware of the fact that QubesOS offers one of the best way to compartmentalize and run VMs in a very efficient way. QubesOS includes Whonix which is used by almost everyone here. While running Whonix on QubesOS is the most secure way, there are some limitations and features that Whonix cannot offer when you are running it on QubesOS. Some of which are outlined below:

1. Kloak is not supported. Keystroke Deanonymization is a technique used by adversaries to identify the typing style of users. For example, how long the breaks/pauses are in typing, how many errors are made and the most common errors produced, whether they are likely right or left-handed, etc.

2. Strong Linux User Account Separation / Protection against Bruteforcing Linux User Account Passwords is broken. This feature is self-explanatory. It prevents brute force attacks and implements mitigations like lock user accounts after 50 failed login attempts using faillock until password unlock procedure is required, etc. (Read more about it here)

3. TCP ISN CPU Information Leak Protection not supported. Short for tridad, it is used to prevent CPU information leakage. The Linux kernel has a side-channel information leak bug. It is leaked in any outgoing traffic. This can allow side-channel attacks because sensitive information about a system's CPU activity is leaked. Research has demonstrated that it can be used for de-anonymization of location-hidden services. (Research Paper: https://www.cl.cam.ac.uk/~sjm217/papers/ccs06hotornot.pdf)

4. No plans for implementing Linux Kernel Runtime Guard (LKRG). LKRG performs runtime integrity checking of the Linux kernel and detection of security vulnerability exploits against the kernel. Basically a crucial kernel hardening feature. (Read more here)

That's all I could find. All of them are default in Non-QubesOS Whonix. There are some other things you might wanna take a look regarding security and privacy which are not enabled in QubesOS by default. QubesOS

community can be a good start and has a good list of things you could implement to improve your overall setup (QubesOS Community)

7 comments

/u/Paris A

As a basically religious user of Qubes I'm going chip in here and break some of the misinformation in this post.

Qubes is a compartmentalized focused OS. It does the compartmentalization process with the Xen hypervisor. The Xen hypervisor runs on the bare-metal layer. It doesn't need a kernel to run because itself is just running on the host's hardware. This is different from a lightweight container solution by providing a hardware level full virtualization resulting in more security separation overall. KVM has full virtualization support and if you use VirtualBox with properly supported hardware you generally will be running with it too. There is however a difference. KVM is baked into the Linux kernel level while Zen is separate from the host kernel. The reason why you would want something like LKRG is to secure the Linux kernel's KVM hooks against exploits which can compromise the underlining virtualization. Zen doesn't need that.

In fact all of your limitations outlined have nothing to do with the difference of the virtualization layer. The first one deals with a human element of how they type and how websites or applications can track that to correlate things. The reason why Qubes doesn't support Kloak is quite simple. When you click away your keyboard and mouse pointer basically freezes on the deselected Qube. Like someone got up and walked away generally but also played a bit with the keyboard plugs. This could mess up how Kloak detects input and output and cause bugs in their C code. If you want you can still install it in a HVM and have it run if you are that paranoid. But by that point you should already have javascript off in your browser and this identitifcation vector becomes basically nonexistent.

The second one makes no sense to me at all. If you want you can set up the Qubes to require password authentication. But you shouldn't be working within template qubes that keeps state anyway. You just make an AppVM for the application you want to run, set it up, and then run it. If the VM gets compromised under use you just close it and open it up again. It will pull the non-compromised template state. By the verify design you assume the AppVM is compromised but it doesn't matter because it's separated from everything else you could care about.

The third one makes little sense either in the case of difference between Qubes and Whonix on KVM. TCP ISN CPU Information is standardized on the kernel layer. If you change the way you are handling this information on the kernel level you would stand out over everyone. If this somehow was a serious thing it would have far reaching consequences. You can also install some kernel ISN masking modules if you care about it even in template Qubes if you care enough. We have sdwdate systems in Qubes Whonix to correct for time skew as well. Let alone if you are running an onion service you should be running on servers which can be moved, burned, and otherwise without any

personal information leak on your part. I also think the latest kernels have hardened the way the ISN is generated since this was researched well over 16 years ago. It just isn't an issue in my view anymore.

/u/decaptchamyass

It's actually Xen, not Zen. And the things I have outlined are just facts. Instead of "debunking misinformation" which seems incorrect, you could have just said "I will elaborate more on these topics." I have already talked to Patrick about this and he doesn't seem to have a different opinion.

Are you aware that even without JS, websites are able to fingerprint? The same way, it is very much possible to track the keystrokes without JS. Disabling JS just reduces some of the attack surface but in no way does it mean that you are immune to every attack vector.

The second one is not just about "Password Authentication". It's more than that. Read the documentation that I have linked.

/u/Paris A

Oh yes. I keep fucking up that name because I always say Qubes brings me Zen.

Look, facts put in a way to scare people when there isn't any concern causes harm. Without JavaScript on a website there is no realistic way to track keystrokes on the page. Fingerprinting of the browser is also not a real concern on a Qubes system because it's not like you are using a different Tor browser vs a regular Whonix Workstation.

When it comes to password authentication on Qubes AppVM there is no point in isolating user accounts. This is because all user data is already accessible from the user account. With Qubes, there are no benefits for an attacker if they would escalate to root. It's not like they could install rootkits as the root of the filesystem are lost on every AppVM start. The entire idea is to compartmentalize everything assuming that any AppVM can be fully compromised after the boot. In the case it is, a simple reboot of the VM restores the non-compromised state. So no it doesn't need to just be about password authentication but it simple isn't a concern. There is literally no point in doing something like the documentation has outlined in your link on a Qubes AppVM. Secure by default. No password needed. Separation comes from not user accounts or permissions but completely different VMs.

/u/We_Are_9000 Paranoia Level

The whole point of using a VM is too prevent any leaks, that is what a sandbox does. The isolation inside the VM prevents man in the middle attacks, so how could anything be leaked????

/u/Yamaca

Whonix is more for your network security more than anything else.

/u/Junctionman1

Damn man... more stuff for me to research. Can someone explain what QubesOSis in a quick brief explanation and why someone would want to use such a thing?

This book will not cover any of the hundreds of Linux variants in any detail, but will provide some general information in the following pages.

Additional Linux References:

Securing Debian Manual 3.19

This document describes security in the Debian operating system. Starting with the process of securing and hardening the default Debian GNU/Linux distribution installation.

hxxps://www.debian.org/doc/manuals/securing-debian-manual/index.en.html

Some Simple? Whonix Security Hardening Steps

This reads like a Russian novel...written in Greek

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion-/post/36134b759eacb6ddc8c8

Other Linux distros (but not all 270)

Sick of Windows but can't afford a Mac? Consult our cynic's guide to desktop Linux

For your consideration: A reasonable list of the least bad distros

Liam Proven in Prague Tue 31 May 2022 // 10:15 UTC

264 comment bubble on white

It is a truth universally acknowledged that all operating systems suck. Some just suck less than others.

It is also a comment under pretty much every Reg article on Linux that there are too many to choose from and that it's impossible to know which one to try. So we thought we'd simplify things for you by listing how and in which ways the different options suck.

This would be an impossibly long list if we looked at all of them since Distrowatch currently lists 270. So we need to thin the herd a bit.

If you're interested in a comparison like this, you probably don't have a favorite already.

0. Tiny obscure distros. All of them.

Avoid all the niche efforts. Here's why. Firstly, they're small. Not many people use them, so you'll have difficulty finding people to ask for help. Secondly, third-party hardware and software probably won't work out of the box, and if you ask the vendor for help, whether it's a game or a graphics card or a printer, they won't have heard of Ultimate SuperL33tOS version Pi. Game over. Just don't. Stick to the mainstream.

1. ChromeOS Flex

The year of Linux on the desktop came and went, and nobody noticed – maybe because it doesn't say "Linux" on it. ChromeOS only runs on ChromeBooks and ChromeBoxes, but they outsold Macs for a while before the pandemic. "Flex" is the version for ordinary PCs, presumably named because it's what puny $1.5 trillion Google is doing. ChromeOS Flex works great, because it only does one thing: browse the web. You can't install apps, not even Android ones: only official kit does that. You can run Debian containers: if you know what that means, go run Debian. If you don't know what that means, trust us, you don't want to.

2. Ubuntu

"Ubuntu is an ancient African word that means I can't configure Debian.*"

Ubuntu started out as an effort to displace Windows from the number one consumer OS spot by making a Linux that was easier to install and run. It worked. So Microsoft threatened to sue because it looked a bit like Windows if you squinted, and the whole thing fell apart. Ubuntu decided that if it was dodgy to look Windows-like, it would look like Mac OS X instead. Then it went back to GNOME again.

Ubuntu used to be the obvious choice, but it took its eye off the "for human beings" ball (great explanation there, folks) to grab at servers – which, to be fair, is where the money is – and it shows. When it gave up on all its in-house stuff, it kept Snap, its universal app-packaging format that no other distro uses. They work, but they gobble disk space and make bootup slower. If you just want to get on with using it rather than fiddling and fighting, try Ubuntu MATE or Xubuntu, but then our warning about niche distros applies.

3. Linux Mint

Mint is an Ubuntu remix with knobs on. It was an also-ran for years, but when Ubuntu went all Mac-like it saw its chance and grabbed it – along with the number one spot in the charts. It dispenses with some of the questionable bits of recent Ubuntu, such as GNOME and Snaps, but replaces them with dodgy bits of its own, such as a confusing choice of not one, not two, but three Windows-like desktops, and overly cautious approaches to updates and upgrades.

4. Debian

Debian is the daddy of free distros, and the one that invented the idea of a packaging tool that automatically installs dependencies. It's easier than it used to be, but mired in politics. It's sort of like Ubuntu, but more out of date, harder to install, and with fewer drivers. If that sounds just your sort of thing, go for it.

5. Fedora

Red Hat made billions by switching from a free distro to selling an exceptionally boring corporate-server one. This upset the freeloaders. Fedora is the bone Red Hat threw over the fence to them. It's matured into something comparable to Ubuntu, but without the stable releases. You'll be upgrading twice a year, unless you put it off, cross your fingers, and hope that skipping every other version works. Probably not worth the effort unless your day job is trying to stop RHEL boxes falling over, or trying to build code that runs on RHEL boxes without falling over.

6. openSUSE

A whole six months older than Red Hat, SUSE is another vendor of expensive enterprise distros which tosses freebies over the wall. Its innovative solution to Fedora's no-stable-releases issue is to have two different distros. One, "Leap", is synchronized with the paid-for SUSE Linux Enterprise – which is to say it has a painfully slow release cycle. The other, "Tumbleweed", has a rolling release model, which means the exciting potential of breaking changes every single day.

To compensate, it uses Btrfs and snapshots to make it easy to roll back updates – but the package manager doesn't know about snapshots, or Btrfs's famed inability to tell you how much free disk space you have, so it occasionally fills up your file system and corrupts it. Frustrated

boredom or cringing terror, it's your choice: have a lot of fun!

SUSE and KDE are both German and it's been the best distro for KDE approximately forever. Demonstrating its deep understanding of the Linux world, Novell bought SUSE, then bought GNOME vendor Ximian, then forced them into an arranged marriage. Now SLE doesn't even offer KDE as an option.

7. A RHEL spin-off

IBM subsidiary Red Hat remains the titan of the Linux world. Specifically, Cronus, who ate his own children. So it bought CentOS, then killed it, as it did with CoreOS.

Freely mixing classical allusions, this has resulted in a hydra situation: many more heads have sprouted. If Fedora is an alpha release of RHEL, CentOS Stream is a sort of beta.

Unity and Trinity: New releases for forks of abandoned Linux desktops

Debian faces firmware furor from FOSS freedom fighters

Why the Linux desktop is the best desktop

Zorin OS 16 beta claims largest built-in app library 'of any open source desktop ever'

Why make games for Linux if they don't sell? Because the nerds are just grateful to get something that works

Or there are Rocky Linux and AlmaLinux, which are RHEL with the serial numbers filed off. Ideal for prototyping stuff you'll later deploy on RHEL, or if you're upskilling for a job in a Red Hat shop, or if you just can't afford the real thing. And there's Oracle if you feel that it looks more trustworthy than the Hat these days.

For your own laptop, these are all perennially a bit behind the times: just what you want if you're a big enterprise, but not if you're running it at home.

8. Pop!_OS

Pop!_OS is arguably one of the most interesting Ubuntu remixes. Saying that, bear in mind the famous line about living in interesting times, and that a motto of the open-source world is to move fast and break things. If you must, put it on a brand-new PC and don't try to dual-boot. Also, remember what we said about niche distros, which applies to all the Ubuntu remixes.

9. Arch Linux

Finally we come to the 10th entry in our list, because Unix people are difficult and like to count from zero. As one of the original rolling-release distros, Arch is the embodiment of moving fast and breaking things. Great if you're a hobbyist or a gamer, not so good if you have a job to do. This also applies to its offspring such as EndeavourOS, Manjaro, and Garuda.

Conclusion

There are loads of worthy entries that did not make our snarky and (honestly!) affectionate list. This was a top 10 for a reason: everything on this list is one of the leading Linuxes out there, and every distro here is a good solid contender in its own way.

The world of free software came into existence because people have very strong feelings about the Right Way To Do Things, and as a result, it both has a strong sense of community and deeply, fundamentally opposed factions, such as the Debianistas versus the Hatters. And that's without going into the desktop or editor wars.

There are lots of others with completely valid reasons for existence, too. The Reg FOSS desk mainly runs a distro that's not in this list at all.

It's all good. Really. ®

* Jokes aside, Ubuntu is an Nguni language (Ndebele, Xhosa, Zulu) word that is broader concept philosophically in southern Africa, to do with respect, kindness and generosity in a community. The idea is that it is only through pro-social interactions with other people that you are a human being: "umuntu ngumuntu ngabantu" – "I am because you are."

https://www.theregister.com/2022/05/31/the_cynics_guide_to_linux/

Kodachi (Japanese for small sword)

Kodachi is a free Debian based Operating System designed specially for security, anonymity and privacy. It has built in anonymity, cryptography and anti forensics solutions. If compared with others, its a better alternative for its competitor Operating Systems like Tails and Qubes. It has a complete suite of tools and utilities that one needs to secure his privacy and anonymity on the internet.

When Kodachi boots up, it changes your MAC Address, establishes TOR (The Onion Routing) connection through a paid VPN and all of the internet traffic has to go through TOR plus VPN with DNS encryption. Also it changes your MAC Address regularly after a while to avoid detection and tracking on the internet.

Kodachi runs on Live USB, CD, DVD and can be used with USB persistence, also it can be installed on Hard Disk Drive but that's not recommended. Kodachi is entirely anti forensics, it leaves no traces of your activity on host system and can't be traced back. It also has wipe RAM option in Panic Room Panel to clear Temporary Memory.

https://linuxhint.com/kodachi_os_review/

There was some discussion about this OS on dread OpSec.

/u/We_Are_9000 Paranoia Level

Well, if these fools would take the time to learn real OPSEC & use it everyday, there is nothing to fear on the surface web.

If you guys have not added Kodachi to your OS list, you really need to, it makes Tails look like a bowl of cold oatmeal. You should check out its versions of Firefox, total lockout of the so called things to fear.

Where did common sense go? Because that is a very important part of staying safe online, surface web or darknet.

/u/yosegi

I documented myself and I tested kodachi unless I am mistaken kodachi is dangerous, I made a post /post/4e47647666965d811e05

if I summarize kodachi obliges to use his vpn before tor then obliges to use his dns after tor

moreover in their condition kodachi declares to collect your ip address as well as your hardware address as quoted below

"I pay monthly rent to run the VPS nodes and utilize them for VPN which is provided to you, I do not collect ANY data or store ANY information (Logs) that belongs to the user except the hardware ID (hash) and connected IP address (VPN IP) that has to be sent automatically when your PC establishes a connection to the VPN. This information will only be used to banned you from the VPN nodes if you have abused the bandwidth or I received complaints of hosting torrent files. If that is the case you will be banned permanently Kodachi is provided for anonymous surfing and not for heavy daily file and movie downloads.If you think you have been banned by mistake please send me your Hardware-ID via contact Discord and yes you can use your own VPN then no HWID will be sent to the server."

I confess to not understanding to see kodachi regularly quote as a good OS

whonix is a very good compromise and remains accessible to use qubes if we have the will to understand its operating logic, I find it less complex than we think

/u/Pygmalion Vendor Opsec

Kodachi is fucked because it is based on a distro that will no longer receive security updates soon.

Other than that it's really good, but yea, it will be out of date soon unless they step up their gears.

/u/We_Are_9000 Paranoia Level

I can't see that upgrade not happening, its the same as not updating Tor itself. I'm certain that shooting themselves in the foot is not on the table.

/u/alwaysfire

"If you guys have not added Kodachi to your OS list, you really need to, it makes Tails look like a bowl of cold oatmeal."

In terms of "features", Kodachi does make Tails look like a bowl of oatmeal. However, with more features comes more attack vector, more possibility for human error, and more possibilies for bugs, misconfigurations, etc. Kodachi is also produced by one single developer, who stores his public pgp signing key in an impossibly hard to find place. Placing all that trust in one single dev isn't a great idea. Without many eyes and oversight, it's prone to have many more security issues than tails. It also uses the developers free vpn service as a default vpn. Using any free VPN is a bad idea, and bad for opsec. I agree that kodachi has many more features than tails, but I strongly dissagree that It should be used over tails. Tails is idot proof and kodachi is not. Theres a lot that could go wrong with kodachi in terms of opsec.

How to prepare Windows 7 Ultimate 64 bit for the Internet in general and also the DW

This really needs to be a machine dedicated to the DW only.

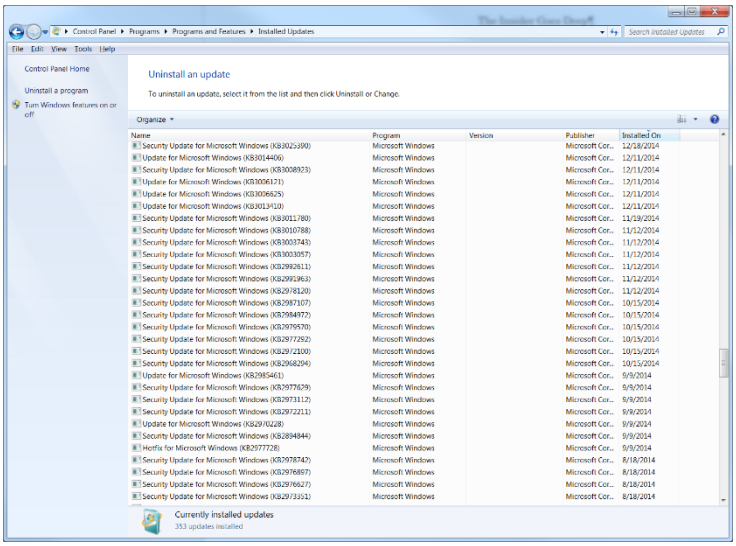
Do not even think about using Windows 8, 10, or 11. They are far too chatty across the Internet and incorporate telemetry and keylogging that can make you easy to identify. There are however some tips that follow.

With Windows 7, starting in 2014, all updates especially those marked as Security, are suspect. See my book, The Cozening, for more detail on this. These updates are mostly for preparation for Windows 10 and incorporate the MS belief that they are allowed to control your computer since you are using their software, whether you bought it or not.

Start with a clean install of Windows 7 64-bit Service Pack 1, build 7601.

Do a custom install and eliminate anything unnecessary to install. Running this inside of a Virtual Machine (Virtual Box) or not is up to you, but not necessary in my experience. It really depends or how comprehensive your backup strategy and OpSec are.

Your updates should basically stop at SP1. Some .net framework updates may need to be installed.


Control Panel ▸ Programs ▸ Programs and Features ▸ Installed Updates
File Edit View Tools Help
Control Panel Home
Uninstall a program
Turn Windows features on or off
Uninstall an update
To uninstall an update, select it from the list and then click Uninstall or Change.
Organize
Name
Program
Version
Publisher
Installed On
Currently installed updates

You should eliminate (uninstall) or spay and neuter all Adobe products if you can as they are chatty as well. Since I need pdf's for these books, I control it with my Zone Alarm firewall and the other hardening software mentioned elsewhere here.

Do not install any software that is not absolutely necessary for your purposes.

Install the Tor bundle. (although some say not to use this because it may be compromised and to install manually instead)

Aside from software updates and telemetry, where does Windows leak IP and ID info?

Assume a tuned and hardened Windows 7 bare bones system, updates off since SP1, updates off in registry and disabled. No Win10/11 so No Cortana, No OneDrive.

- **Tor updated and security at Strict (javascript off)**
- **Tor email only**
- **Ahmia search only**
- **TMAC for changing (spoofing) your MAC address**
- **Use Windows Task Scheduler to disable or delete all unnecessary and intrusive scheduled tasks**
- **Download and use Sysinternals Process Explorer to shut down and disable all unnecessary processes.**
- **Use Winaero Tweaker by Sergey Tkachenko , a very comprehensive, powerful, small and free tool to make Windows behave and to look like however you want it to. Well within reason anyway. You can't make it Win7 SP2, or what Win8 should have been. It will however give you back the control that MS took away over the years.**
- **Synchronize with an Internet time server off (should not be necessary behind a VPN)**
- **Windows NCSI communication across the Internet, EnableActiveProbing OFF (registry edit) https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc766017(v=ws.10)?redirectedfrom=MSDN**
- **Paid VPN (passes IP leaks, DNS leaks and WebRTC leaks)**
- **Zone Alarm for firewall and AV (free version is fine)**
- **Norton Ghost or other software for image backups to network and/or external drives**

- **SpyShelter anti-keyboard logger installed**
- **Spybot Anti-Beacon installed (kills telemetry)**
- **https://www.safer-networking.org/products/spybot-anti-beacon/**
- **BleachBit for cleaning your system and keeping it clean**
- **PGP Tools for encryption and decryption**
- **7-Zip for creating zip files**
- **eBook reader software**
- **Quality updated gaming router with NAT**
- **Wireshark to analyze packet flow install Wireshark and set it to capture from your wired or Wi-Fi network interface.**

https://winaerotweaker.com

More info at:

https://www.tcw.org/lefty/Short%20Stories/Configure_-_The_Windows_7_To_Work_Options.pdf

https://www.tcw.org/lefty/Short%20Stories/Configure-%20Windows%208%20To%20Work,%20Kinda.pdf

More Tools for Windows 7/8/10/11:
Private WinTen
Blackbird v6
O&O ShutUp10++
WPD - Windows Privacy Dashboard
WindowsSpyBlocker
Spybot Anti-Beacon v3.5
W10Privacy
Privatezilla
SharpApp
Debotnet
Disable Windows 10 Tracking v3.2.3
Destroy Windows 10 Spying
Win10 Spy Disabler
DisableWinTracking
Privacy Repairer
Ashampoo AntiSpy for Windows 10
Windows Privacy Dashboard
WindowsSpyBlocker

Windows 10/11…do not despair as they are not completely hopeless but do not use on the DW

Note: You will need some skills to do this, either achieved in the process or previously hard earned, but anything really worth doing is bound to be hard. The cost is money is basically zero in dollars, depending on what you PayPal donate to the people who wrote these programs, which you should do. To experiment with, use a machine that you don't need for anything else. If you must, at least install free VMware player software and install it in a virtual machine.

There is a little know version of Win 10 called LTSB (Long Term Service Branch), available from 2016-2019 It is an add-on to an SA Win10 Enterprise license which is not available to most people. It uses an SA Enterprise key for activation. It was primarily intended for factory machinery and kiosks. Some software may not run on this version. None are known to me at this point.

Its primary features are what is **not** there:

1. No Cortana,
2. No MS Store
3. No Telemetry
4. No Crappy Xaml Apps
5. No Forced Updates
6. No Edge Browser
7. No Xbox

But since it is still Windows 10 which is a devolved, stripped down, and perverted version of the Windows we all knew and loved since 1988, it needs some serious work to make it usable. After all, Win10 was designed primarily for Mobile and Cloud computing for phones and tablets. Apparently no one is supposed to be using desktops or non-touchscreen laptops anymore according to MS.

Download an MS evaluation copy to install and play with

This is the first thing your should do going down this path. It will not activate and will work for 90 days and then quit. Before that time however you will have figured out if this is workable for you or not.

Downloads come from the sites listed. Modifications will be in the following areas:

- **Classic Shell** **(www.classicshell.net)**

  Download, install and configure this alternate interface to your preferences.

- **Winaero** **(www.winaero.com)**

  Download, install and configure Winaero Tweaker. It is pretty amazing on what it will let you do the reconfigure Win10. It's almost daunting how many settings it provides access to. This program reminds me of all the good software I have used over the years and we don't have now, in this silly mobile app-centric phone and cloudy world.

  https://winaerotweaker.com

- **Aero Glass for Win8.x** **(**www.glass8.eu)

  Works on Win10 based on your current version.

- **Vista Icons** **(https://vista-icon-pack.en.uptodown.com/windows)**

  You can play like a kid with these.

- **Vista Gadgets** **(https://download.cnet.com/s/gadgets-for-windows-vista/)**

  Be careful where you get these. It's best to be cautious about where you get Gadgets from. Gadgets are as powerful as they are is because they have deep access to your system. Malicious code in a Gadget can truly wreak havoc. cnet.com has been a trusted site for all downloads for many years now.

If you decide this is the right approach for you, do the following:

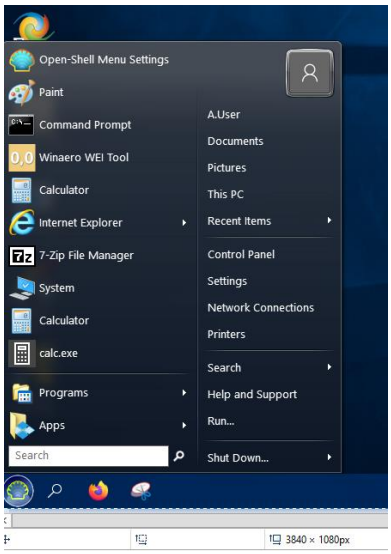
Note: I am not going to walk you through everything step by step with screen shots. (that would be a book that I would need to sell) So some of this you will just need for figure out for yourselves.

- **Download an available .iso and key online to a usb drive or burn to a DVD (some searching will be required to find it)**
- **Scan the .iso with you AV and Malwarebytes**
- **Use 7zip to unpack the .iso to a folder**
- **Scan the unpacked .iso with AV and Malwarebytes**
- **Install Win10 minimally**
- **Scan your hard drive with Kaspersky rootkit finder**

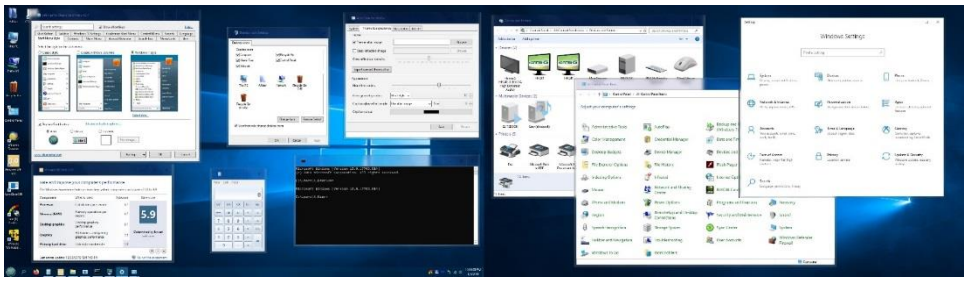
Once you are sure that your install is clean, you can go about reconfiguring it using the software tools as above.

Install Mozilla Firefox and some web browser extensions to keep you from getting tracked and your info stolen while on the Internet. Set the security to Strict. Use DuckDuckGo or StartPage for a search engine that doesn't track you. Use browser extensions to block ads and tracking your browsing history, and use Private Browsing on all sites. You will need to use, train, and update web browser extensions like Privacy Badger, Ghostery, DuckDuckGo Privacy Essentials, and HTTPS Everywhere to block this tracking and personal data theft.

So you can have a Start Menu that looks like this:



And you can make your system desktop look something like this, if you like. (dual screen setup)



More about software.

The many reasons for not upgrading to Window 10/11 include the primitive interface, extensive telemetry, and the poor quality xaml software apps addressed above. One serious reason for not upgrading is software program access and compatibility. I will address this issue here. I will not address hardware compatibility which is another valid reason.

Loss of the Media Center program is a big deal to many, even though Microsoft says that their telemetry shows that hardly anyone used it. Introduced in 2002 on Windows XP and upgraded a bit over time, it was in need of a serious upgrade to support streaming, Blu-Ray media, cable TV tuners, and many other things. This would involve not only designing and writing code, the original program development may have been outsourced, and licensing etc. Remember, Microsoft gutted their software testing department, just before the release of Win10 so the beta Win10 code could be forced on an unsuspecting public.

Microsoft is typically too far out on their skis compared to the rest of the world. They eliminated support for optical disc media early, because everyone was supposed to be using streaming like them. Unfortunately, much of the world does not have their Internet bandwidth to support this. The same is true with this continuous OS updating that strains peoples Internet accounts, not to mention many small local ISP's.

So part of this is being out of touch with reality and some of it is cost, since Windows is no longer their primary source of income and they have since moved on to all this silliness of mobile, probability of data centers, and the illusion of secure clouds.

If you are inclined to try something else for this functionally, try here:

The 5 Best Alternatives to Windows Media Center

https://appuals.com/the-5-best-alternatives-to-windows-media-center/

If you do some desktop publishing, you will notice you now have very few fonts. Typically about 300 on a Windows 7 machine and about 80 on a Win10 LTSB machine. This was another foolish move to make the OS smaller for phones and tablets, and perhaps to save money on licensing. You can get free fonts here:

https://www.1001freefonts.com/

https://www.wfonts.com/

You can also get rid of the crappy App calculator by down loading and installing the old style one, and the old System Configuration and Task Manager via Winaero Tweaker.

VPN's

When to use a VPN?

In a VPN connection, an encrypted tunnel is created that allows an uninterrupted flow of data from your device to a VPN server, which acts as your entry into the public Internet.

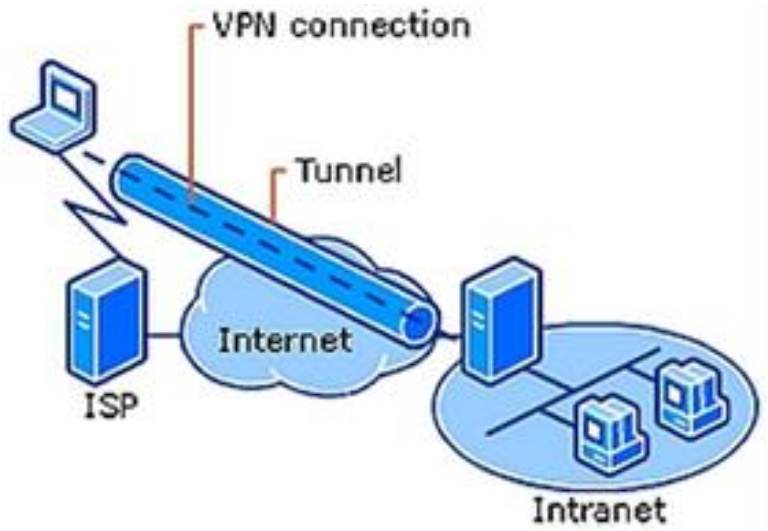
A VPN is capable of providing high speeds and it can successfully meet the needs of our movies buffs and YouTubers. Remember that only your connection is encrypted and not your data, so make sure you are using the SSL protocol while sending some confidential data.

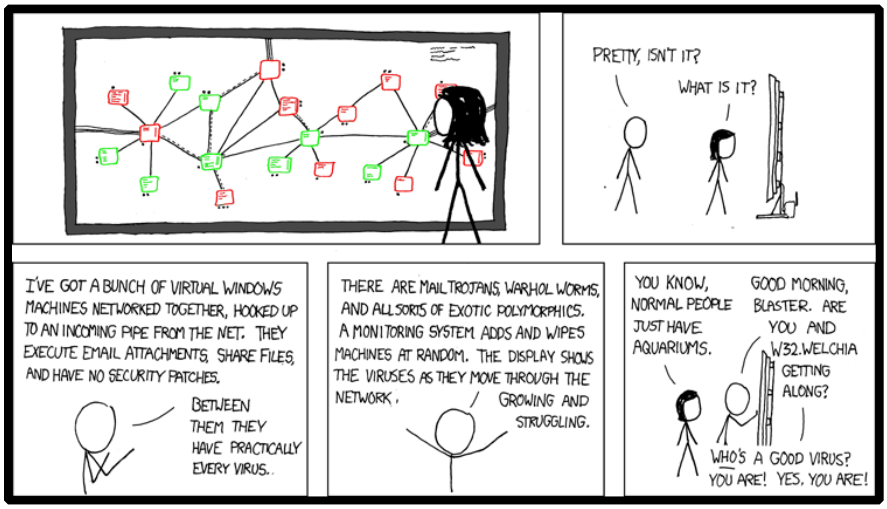
The VPN server has access to all the traffic you have initiated, popular VPN services claim that they do not store any logs. Choose a provider wisely because that claim might be legitimate until a government agency asks them about your existence on their network.

A VPN network can be used in low-risk situations like if you are not accused of some crime that you may or may not have committed, or if you want to hide from various tracking tools on the Internet and simply browse the Internet or download torrents. They are also used to extend a company's private network facilitating the employees to work from a remote location and still have access to the company's resources.

VPN's are also used to extend a company's private network allowing the employees to work from a remote location and still have a secure connection to the company resources.

https://www.zdnet.com/article/best-vpn/




PRETTY, ISN'T IT?
WHAT IS IT?
I'VE GOT A BUNCH OF VIRTUAL WINDOWS MACHINES NETWORKED TOGETHER, HOOKED UP TO AN INCOMING PIPE FROM THE NET. THEY EXECUTE EMAIL ATTACHMENTS, SHARE FILES, AND HAVE NO SECURITY PATCHES.
BETWEEN THEM THEY HAVE PRACTICALLY EVERY VIRUS.
THERE ARE MAIL TROJANS, WARHOL WORMS, AND ALL SORTS OF EXOTIC POLYMORPHICS. A MONITORING SYSTEM ADDS AND WIPES MACHINES AT RANDOM. THE DISPLAY SHOWS THE VIRUSES AS THEY MOVE THROUGH THE NETWORK,
GROWING AND STRUGGLING.
YOU KNOW, NORMAL PEOPLE JUST HAVE AQUARIUMS.
GOOD MORNING, BLASTER. ARE YOU AND W32.WELCHIA GETTING ALONG?
WHO'S A GOOD VIRUS? YOU ARE! YES, YOU ARE!

In a VPN connection, an encrypted tunnel is created that allows an uninterrupted flow of your data from your device to the VPN server, which acts as your entry into the public Internet.

10 advantage of using a VPN

1. Hide your activity from your Internet Service Provider.
2. Protect yourself when using a Wi-Fi hotspot.
3. You get to keep your private searches private.
4. Browse websites without leaving a trace of your identity.
5. Access to streaming, wherever you are.
6. Stay safe from snoopers looking to access your information.
7. Access websites that are not available to an IP addresses geographic location.
8. Access to Internet freedom.
9. You can by-pass surveillance and national internet censorship.
10. You can by-pass school or workplace restrictions.

After much experimenting, the free VPN's started to disconnect and reconnect randomly but yet consistently, and so I gave up on free VPNs and downloaded and installed Express VPN.

And that is all there is to it. So far it is rock solid with no dropouts.

Ok, so after using it for a few days, same problem.

Disconnecting the VPN kills the Internet connection for everything else, unless you leave the application running in the background.

Will try using the VPN full time and see how many Clear Web sites will not work correctly. Although something tells me to switch VPN servers when moving back and forth between Tor and Firefox to avoid detection.

Tools are actually built into the software Help and Support options menus.

Using the WebRTC leak detection site it shows this:

Your ISP can see what websites you visit with the IP Checker.

IP 45.134.22.60 Italy - Cosenza

DNS 162.158.128.186 Cloudflare Italy

Your ExpressVPN IP address

185.198.241.66

Your IP address is secured. Websites cannot use it to identify you.

Location India (via UK)

A DNS leak detector.

When you turn off Enable DNS over HTTPS in Firefox, you get this:

Now No DNS leaks detected

You're using ExpressVPN secure DNS servers.

A WebRTC leak detector.

No WebRTC leak detected

ExpressVPN is protecting you from WebRTC leaks.

IP address	Type	Status
45.134.22.51	Public IPv4	No leak

Note: there is some controversy regarding DNS over HTTPS as to it being effective or not.

There is also a diagnostic tool which will show you your IP path.

Connecting to Italy - Cosenza, ip: 224.58.248.188, protocol: lightway_udp

Client Version: 10.23.0

Client Shared Version: v22.15.0

OS Name: win

OS Version: win6.1.1.7601
Internal diagnostics data:
D01: 397, OK
D02: 397, OK
D03: 396
D04: 4596, OK
D05: 4596, OK
D06: 396
D07: 996, OK
D08: 996, OK
D09: 4596, OK
D10: 996, OK
D11: 996, OK
D12: N, N
D13: www.2spb2qq8pnqmv.net/api
D14: USA - Chicago
D15: auto
D16:
PjA2KGWDvqpmZmZmZmZmZmZmZmZmZmZmZ3ZmZ2Zl
k0dnYRERFIFBIED1MSBwtIBQkLERERSBIBUxIMVAUTSA
UJC2ZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZ
mZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZm
ZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZ
mZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZm
ZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZ
mZmZg==
D17: 1169
D18: 1
Network Lock: enabled, allow access to local devices
DNS leak protection: enabled
IPv6 leak protection: enabled
Selected location: Mexico
2022-04-27T12:29:52.624-0500 Lightway: 1.19.0 libhelium: v1.0.0-10-ga0ce4e0 libxenon: v1.1.0-0-ge67d197 libballoon: 0.10.0
2022-04-27T12:29:52.624-0500 Lightway will connect to 224.58.248.188:37165 using protocol: udp, cipher: aes, mtu: 1500
2022-04-27T12:29:52.624-0500 sndbuf: [8192 -> 1310720]
2022-04-27T12:29:52.624-0500 rcvbuf: [8192 -> 1310720]
2022-04-27T12:29:52.624-0500 Lightway is CONNECTING
2022-04-27T12:29:52.746-0500 Nudging Lightway...
2022-04-27T12:29:52.887-0500 Lightway Initial packet received

2022-04-27T12:29:52.951-0500 Nudging Lightway...
2022-04-27T12:29:53.154-0500 Nudging Lightway...
2022-04-27T12:29:53.170-0500 Authenticating...
Etc. ...

And so it seems that they also honor their privacy commitments.

Rejecting Data Demands, ExpressVPN Removes VPN Servers In India (indianexpress.com) 15

Posted by BeauHD on Thursday June 02, 2022 @05:30PM from the refusing-to-participate dept.

ExpressVPN has removed its servers from India, becoming the first major virtual private network (VPN) provider to do so in the aftermath of the recent cybersecurity rules introduced by the country's cybersecurity agency. The rules require VPN providers to store user data for a period of five years. ExpressVPN said it "refuses to participate in the Indian government's attempts to limit internet freedom." The India Express reports: In a blog post, the British Virgin Island-based company said that with the introduction of the new cybersecurity rules by the Indian Computer Emergency Response Team (CERT-In), it has made a "very straightforward decision to remove our Indian-based VPN servers." While ExpressVPN is the first to pull its services from India, other VPN providers like NordVPN have also taken a similar stance.

The guidelines, released by CERT-In on April 26, asked VPN service providers along with data centers and cloud service providers, to store information such as names, e-mail IDs, contact numbers, and IP addresses (among other things) of their customers for a period of five years. The government said it wants these details to fight cybercrime, but the industry argues that privacy is the main selling points of VPN services, and such a move would be in breach of the privacy cover provided by VPN platforms.

ExpressVPN described the cybersecurity rules as "broad" and "overreaching." "The law is also overreaching and so broad as to open up the window for potential abuse. We believe the damage done by potential misuse of this kind of law far outweighs any benefit that lawmakers claim would come from it," ExpressVPN said. It added that while CERT-In's rules are intended to fight cybercrime, they are "incompatible with the purpose of VPNs, which are designed to keep users' online activity private." Indian users of ExpressVPN will still be able to use its service via "virtual" India servers located in Singapore and the UK. "We will never collect logs of user activity, including no logging of browsing history, traffic destination, data content, or DNS queries. We also never store connection logs, meaning no logs of IP addresses, outgoing VPN IP addresses, connection timestamps, or session durations," the company said.

A t-shirt featuring the illegal code (do not cross a border)

Encryption and PGP

The current lack of privacy on the Internet exposes billions of people to mass surveillance and data breaches, undermining trust in digital services and stifling innovation. Thanks to the failure of governments to ban strong encryption during the original "crypto wars" of the 1990s , open source libraries like OpenSSL created an opening for new services like PayPal, Amazon, and eBay to emerge – which would have been impossible without the end-to-end encryption between browsers and websites needed to secure financial transactions. Today is eerily similar: privacy is undermined by pervasive data collection and centralized monopolies, preventing innovative services and platforms from arising.

https://nymtech.net

In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.

https://en.wikipedia.org/wiki/Encryption

Initially, encrypting messages required using the same tool to encrypt and decrypt making distant messaging difficult or impossible.

Two MIT mathematicians called Whitfield Diffie and Martin Hellman solved this in 1976 with a system they called "public key encryption." Each user is given his own personal cypher system comprised of two "keys," which are different but mathematically related to each other through their relationship to a shared prime number.

The mathematics behind it is complicated, but the idea is simple. It means you can share your "public" key with everyone, and they can use it to encrypt a message into a meaningless jumble that can be decrypted only with your secret "private" key.

Public key encryption transformed the potential uses of encryption, because suddenly people were able to send encrypted messages to each other without having to also exchange a code, and indeed without even having to ever meet at all.

Up until the early nineties, powerful encryption was the sole preserve of governments. The United States had even classed powerful encryption as a "munition" in 1976 and made its export illegal without a license.

There are many different software programs now you can use to encrypt. This is the story of one from an excerpt from one of my previous books The Insider (A Life Inside the Personal Computer)

Cryptology pioneer Phil Zimmermann

Phil Zimmermann was the creator of Pretty Good Privacy PGP. Phil wrote the popular Pretty Good Privacy or PGP program, then made available including its source code, through public FTP[17] for downloading. This was the first widely available

[17] *The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network.*

program to implement public-key cryptography. Shortly thereafter, the software spread uncontrollably via the new wide availability of the Internet.

The first PGP version included an encryption algorithm developed by Zimmermann; that he called Bass-O-Matic[18].

The SNL Bass-O-Matic

After a report from RSA Data Security, Inc., in a licensing dispute regarding use of the RSA algorithm[19] in PGP, the United States Customs Service initiated a criminal investigation of Zimmermann, for allegedly violating the Arms Export Control Act. The United States Government regarded cryptographic software as a munition, and thus was subject to arms trafficking export controls. At that time, the boundary between cryptography permitted "low-strength" and cryptography impermissible "high-strength" for export from the United States; put PGP on the too-strong-to-export side of that boundary. The investigation lasted three years and pretty much destroyed Phil financially and emotionally for a time, but then the case was dropped without the filing of any charges. The boundary for legal export of software was later raised, and now allows PGP to be exported.

The government dropped its case without indictment in early 1996, and Zimmermann founded PGP Inc. to release an updated PGP version. After acquisition by Network Associates (NAI), Zimmermann stayed on as a Senior Fellow. NAI later decided to

---

[18] The name is explained in his comment in the source code: "BassOmatic gets its name from an old Saturday Night Live skit involving a blender and a whole fish. This algorithm does to data what the original Bass-O-Matic did to the fish."

[19] An algorithm is a self-contained sequence of actions. Software algorithms perform calculations, data processing and automated reasoning tasks.

drop the product line, and PGP was reacquired from NAI by a company called the PGP Corporation. Zimmermann then served as a special advisor and consultant. Symantec later acquired the PGP Corporation. Zimmermann is a fellow at the Stanford Law School's Center for Internet and Society. He is a principal designer of the cryptographic key agreement protocol (the “association model”) for the Wireless USB standard.

A 2013 article titled Zimmermann's Law, quoted Zimmermann saying, “The natural flow of technology tends to move in the direction of making surveillance easier, and the ability of computers to track us doubles every eighteen months.” His words became prophetic later that year in the wake of documents released by Edward Snowden, published by Glen Greenwald and others regarding the NSA’s massive surveillance of the American people and others worldwide.

https://en.wikipedia.org/wiki/Export_of_cryptography_-from_the_United_States

This is not good.

The seven -- US, UK, Canada, Australia , New Zealand, India and Japan -- are worried that the use of end-to-end encryption makes it impossible for tech companies to identify dangerous content like terrorist propaganda and attack planning, and makes it harder for police to investigate serious crimes and protect national security.

Tech companies argue that end-to-end encryption protects users' privacy rights, and it to weaken it -- by creating a so-called 'backdoor' that would allow the authorities to look at messages -- would put all sorts of private communications at risk from hackers and force them to decide whether to hand over messages to oppressive regimes. End-to-end encryption makes the tech companies' lives easier, and also allows them to claim the moral high-ground when it comes to privacy.

https://www.zdnet.com/article/the-encryption-war-is-on-again-and-this-time-government-has-a-new-strategy/

Users adopted and tech companies introduced end-to-end encryption, due to governments incepting everyone's data and conversations in the first place. It is indeed rich that governments ask us to trust them again.

OpenPGP

PGP stands for Pretty Good Privacy. The prefix "Open" means it is open standard, so many applications support it.

OpenPGP software uses a combination of strong public-key and symmetric cryptography to provide security services for electronic communications and data storage. These services include confidentiality, key management, authentication, and digital signatures.

For those who want to know more technical details you can start with this article on the Wikipedia website.

https://en.wikipedia.org/wiki/Pretty_Good_Privacy

You will need a public key to add to dread profile for encrypted communication there. Install software and generate key. Add it to your profile.

Note: this application requires Java Runtime Environment 1.8+

Sergey Karpushin https://www.buymeacoffee.com/skarpushind

PGP Tool and Frequently Asked Questions

https://pgptool.github.io/#faq

Once you have added your PGP key to your dread profile you will get this message:

dread PGP Key Verification Message:

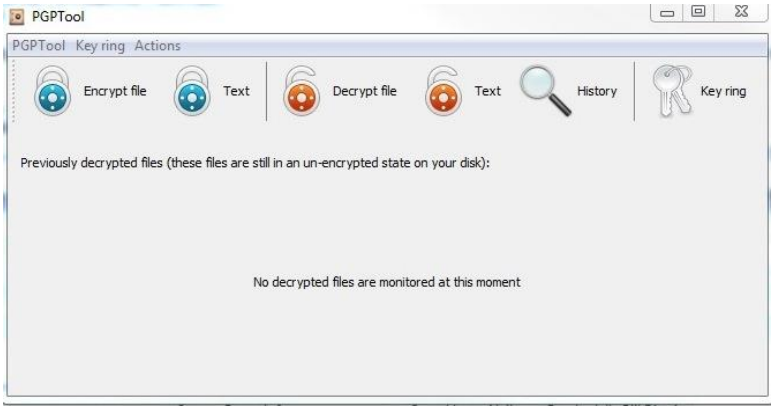
This verification PIN is only valid for

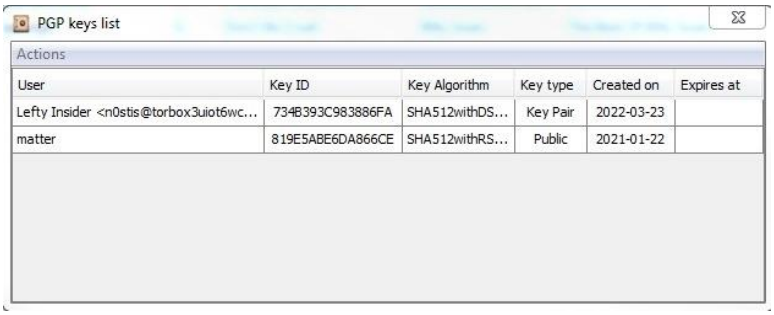
http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv-7jicoxknyazubrad.onion please check the URL in your browser address bar, if it does not match, exit the site now.

PIN: xxxxxxxx

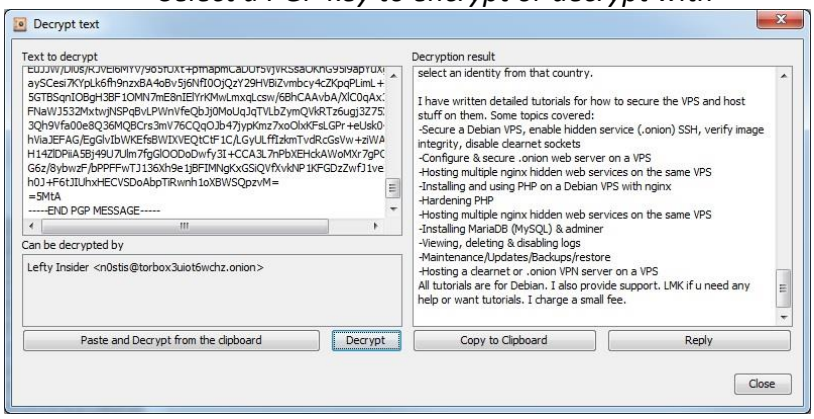
Paste in the above PIN to verify your PGP Key.

You can then decrypt messages with your key and find the key for your recipient and use the senders public key to encrypt a message reply. You can decrypt from the Windows clipboard.

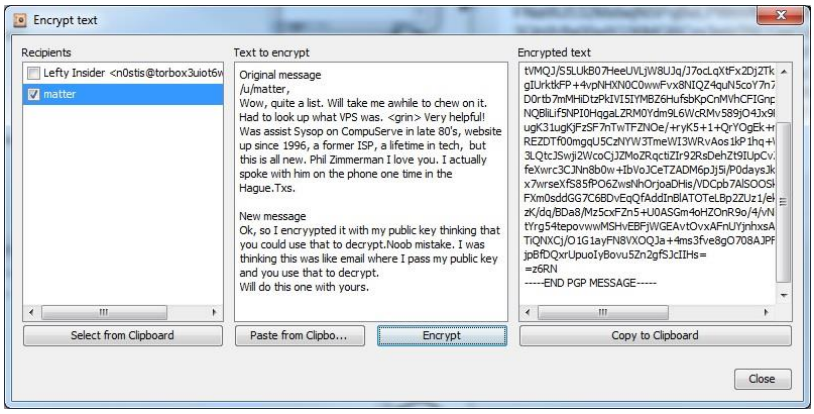




Select a PGP key to encrypt or decrypt with


Decrypt text
Text to decrypt
-----END PGP MESSAGE-----
Can be decrypted by
Lefty Insider <n0stis@torbox3uiot6wchz.onion>
Decryption result
select an identity from that country.
I have written detailed tutorials for how to secure the VPS and host stuff on them. Some topics covered:
-Secure a Debian VPS, enable hidden service (.onion) SSH, verify image integrity, disable clearnet sockets
-Configure & secure .onion web server on a VPS
-Hosting multiple nginx hidden web services on the same VPS
-Installing and using PHP on a Debian VPS with nginx
-Hardening PHP
-Hosting multiple nginx hidden web services on the same VPS
-Installing MariaDB (MySQL) & adminer
-Viewing, deleting & disabling logs
-Maintenance/Updates/Backups/restore
-Hosting a clearnet or .onion VPN server on a VPS
All tutorials are for Debian. I also provide support. LMK if u need any help or want tutorials. I charge a small fee.
Paste and Decrypt from the clipboard
Decrypt
Copy to Clipboard
Reply
Close

Decrypting a message in PGP Tool


Encrypt text
Recipients
Lefty Insider <n0stis@torbox3uiot6w
matter
Text to encrypt
Original message
/u/matter,
Wow, quite a list. Will take me awhile to chew on it. Had to look up what VPS was. <grin> Very helpful! Was assist Sysop on CompuServe in late 80's, website up since 1996, a former ISP, a lifetime in tech, but this is all new. Phil Zimmerman I love you. I actually spoke with him on the phone one time in the Hague.Txs.
New message
Ok, so I encryypted it with my public key thinking that you could use that to decrypt.Noob mistake. I was thinking this was like email where I pass my public key and you use that to decrypt.
Will do this one with yours.
Encrypted text
tVMQJ/S5LUkB07HeeUVLjW8UJq/J7ocLqXtFx2Dj2Tk
gIUrktkFP+4vpNHXN0C0wwFvx8NIQZ4quN5coY7n7
D0rtb7mMHiDtzPkIVI5IYMBZ6HufsbKpCnMVhCFIGnp
NQBliLif5NPI0HqgaLZRM0Ydm9L6WcRMv589jO4Jx9l
ugK31ugKjFzSF7nTwTFZNOe/+ryK5+1+QrYOgEk+r
REZDTf00mgqU5CzNYW3TmeWI3WRvAos1kP1hq+W
3LQtcJSwji2WcoCjJZMoZRqctiZIr92RsDehZt9IUpCv
feXwrc3CJNn8b0w+IbVoJCeTZADM6pJj5i/P0daysJk
x7wrseXfS85fPO6ZwsNhOrjoaDHis/VDCpb7AlSOOS
FXm0sddGG7C6BDvEqQfAddInBlATOTeLBp2ZUz1/e
zK/dq/BDa8/Mz5cxFZn5+U0ASGm4oHZOnR9o/4/vN
tYrg54tepovwwMSHvEBFjWGEAvtOvxAFnUYjnhxsA
TiQNXCj/O1G1ayFN8VXOQJa+4ms3fve8gO708AJPF
jpBfDQxrUpuoIyBovu5Zn2gfSJcIIHs=
=z6RN
-----END PGP MESSAGE-----
Select from Clipboard
Paste from Clipbo...
Encrypt
Copy to Clipboard
Close

Encrypting a message in PGP Tool

Note: Do not make a noob mistake and encrypt a Reply with your own key rather than the recipients key.

/u/matter

Can't read that. Make sure u use my public key to encrypt the message.

(I had used my public key, rookie (noob) mistake.

/u/n0stis

Wow, quite a list. Will take me awhile to chew on it. Had to look up what VPS was. <grin> This was very helpful.

Was assist Sysop on CompuServe in late 80's, had a website up in 1996, was an ISP, and a lifetime in tech, but this is all new. Txs.

/u/matter encrypted message:

-----BEGIN PGP MESSAGE-----
Version: BCPG v1.63

hQEMA4GeWr5tqGbOAQf/QdQGGeZze32w95KjwsKFlWB8diAxgwBcv
KAQzRTq84OS
tVMQJ/S5LUkB07HeeUVLjW8UJq/J7ocLqXtFx2Dj2TkedDZ20apayUV
+0AA1qn72
gIUrktkFP+4vpNHXN0C0wwFvx8NIQZ4quN5coY7n7KZGp7X297NpQ
XbtRqdoyVRZ
D0rtb7mMHiDtzPkIVI5IYMBZ6HufsbKpCnMVhCFIGnpei7/OT5gKF/Ls1
R00WJPJ
NQBliLif5NPI0HqgaLZRM0Ydm9L6WcRMv589jO4Jx9RweOL50ohUF
NaKeWV9Np2e
ugK31ugKjFzSF7nTwTFZNOe/+ryK5+1+QrYOgEk+rtLA5QE9xJHR6O
szb18q14V8
REZDTf00mgqU5CzNYW3TmeWI3WRvAos1kP1hq+WJ49ULkZQ7LV

5qDPMroTwQzSXk
3LQtcJSwji2WcoCjJZMoZRqctiZIr92RsDehZt9IUpCvZ6YQ7pvqMylt1HOKtFoH
feXwrc3CJNn8b0w+IbVoJCeTZADM6pJj5i/P0daysJkJ/9rFSS9wk3znWRpbpTuZ
x7wrseXfS85fPO6ZwsNhOrjoaDHis/VDCpb7AlSOOSk4rsmninqizQ7IGhTL0X1N
FXm0sddGG7C6BDvEqQfAddInBlATOTeLBp2ZUz1/ekOwtvBxUJ6OdKME/NvHnjGD
zK/dq/BDa8/Mz5cxFZn5+U0ASGm4oHZOnR9o/4/vNlIqqHkCqJjgkfuuhvmPLOTl
tYrg54tepovwwMSHvEBFjWGEAvtOvxAFnUYjnhxsAGLxcMVtN3vfQWmBEOJPwxLi
TiQNXCj/O1G1ayFN8VXOQJa+4ms3fve8gO708AJPFvDugGomCgn2PZ5Rq2tXWeWh
jpBfDQxrUpuoIyBovu5Zn2gfSJcIIHs=
=z6RN
-----END PGP MESSAGE-----

/u/matter reply decrypted it was:

I use some of these for VPS hosting

https://pq.hosting/en/
https://alexhost.com/vps/
https://cryptoho.st (https://cryptohost.org)
https://vpsbg.eu
https://evolution-host.com
https://signaltransmitter.de
https://buyvm.net
https://koddos.net
http://www.iq.pl
https://www.privex.io/tor-exit-policy/
http://www.portlane.com
http://urdn.com.ua
https://www.psychz.net
https://www.vpsbg.eu/en/
http://www.pulseservers.com
https://www.netcup.de
https://www.trilightzone.org
https://www.xmrvps.com
https://ablative.hosting
https://ablative.hosting/shared-single-hop-onion-hosting
https://anycolo.net
https://flokinet.is
https://www.swisslayer.com
https://www.epio.host
https://5wire.co.uk

https://userbase.com
https://nicevps.net
https://cryptwerk.com
https://host-world.com/monero-vps
https://abacohosting.com
https://qhoster.com
https://whattheserver.com
https://codify.global
https://www.superbytehosting.com
https://www.superbithost.com
https://www.nexwave.ca
https://www.hostingssi.com
https://blazinhosting.net
https://web.laweitech.com
https://1984hosting.com
https://www.snel.com
https://njal.la
http://njallalafimoej5i4eg7vlnqjvmb6zhdh27qxcatdn647jtwwwui3nad.onion
https://www.bacloud.com
https://cryptofibers.com
https://sporestack.com
https://www.99stack.com
https://radwebhosting.com
https://packetpoint.ca
https://www.serverwhere.com
https://hosthavoc.com
https://abacohosting.com
https://coinhost.io
https://www.bacloud.com
https://www.superbytehosting.com
https://bitvps.com
https://1gbits.com
https://bithost.io
https://airvpn.org
https://builderra.com
https://impreza.host/services/tor-hosting/
https://ipxcore.com
https://orangewebsite.com
https://coin.host

Even more: https://www.bitcoin-vps.com/

Create a new email account to use during sign up. Use Tor a friendly email host like one of these:
https://sector.city
https://elude.in
https://cock.li
https://mailfence.com

DM me for invite code if u need.

Check what country your tor exit node is in (www.whatismyip.com) Use a fake identity generator like https://www.fakenamegenerator.com and select an identity from that country.

I have written detailed tutorials for how to secure the VPS and host stuff on them. Some topics covered:

-Secure a Debian VPS, enable hidden service (.onion) SSH, verify image integrity, disable clearnet sockets

-Configure & secure .onion web server on a VPS

-Hosting multiple nginx hidden web services on the same VPS

-Installing and using PHP on a Debian VPS with nginx

-Hardening PHP

-Hosting multiple nginx hidden web services on the same VPS

-Installing MariaDB (MySQL) & adminer

-Viewing, deleting & disabling logs

-Maintenance/Updates/Backups/restore

-Hosting a clearnet or .onion VPN server on a VPS

All tutorials are for Debian. I also provide support. LMK if u need any help or want tutorials. I charge a small fee.

Even more: https://www.bitcoin-vps.com/

Create a new email account to use during sign up. Use Tor a friendly email host like one of these:

https://sector.city

https://elude.in

https://cock.li

https://mailfence.com

DM me for invite code if u need.

Check what country your tor exit node is in (www.whatismyip.com) *Use a fake identity generator like* https://www.fakenamegenerator.com *and select an identity from that country.*

I have written detailed tutorials for how to secure the VPS and host stuff on them. Some topics covered:

-Secure a Debian VPS, enable hidden service (.onion) SSH, verify image integrity, disable Clearnet sockets

-Configure & secure .onion web server on a VPS

-Hosting multiple nginx hidden web services on the same VPS

-Installing and using PHP on a Debian VPS with nginx

-Hardening PHP

-Hosting multiple nginx hidden web services on the same VPS

-Installing MariaDB (MySQL) & adminer

-Viewing, deleting & disabling logs

-Maintenance/Updates/Backups/restore

-Hosting a Clearnet or .onion VPN server on a VPS

All tutorials are for Debian. I also provide support. LMK if u need any help or want tutorials. I charge a small fee.

GnuPG

GnuPG (more commonly known as GPG) is another implementation of a standard known as PGP (Pretty Good Privacy). It uses a system of "public" and "private" keys for the encryption and signing of messages or data.

Overview

GnuPG is a hybrid-encryption software program because it uses a combination of conventional symmetric-key cryptography for speed, and public-key cryptography for ease of secure key exchange, typically by using the recipient's public key to encrypt a session key which is used only once. This mode of operation is part of the OpenPGP standard and has been part of PGP from its first version.

GNU Privacy Guard (GnuPG or GPG) is a free-software replacement for Symantec's PGP cryptographic software suite. The software is compliant with RFC 4880, the IETF standards-track specification of OpenPGP. Modern versions of PGP are interoperable with GnuPG and other OpenPGP-compliant systems.

GnuPG is part of the GNU Project and received major funding from the German government in 1999.

https://en.wikipedia.org/wiki/GNU_Privacy_Guard

https://gnupg.org/blog/20220102-a-new-future-for-gnupg.html

Canary

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256
Published by: xD500
Published on: 20-03-2022
Next, Publish: 20-04-2022
I am xD500, Admin of Big Bear escrow service.
I am in control of Big Bear PGP Key.
I will update this canary every 20th in month.

-----BEGIN PGP SIGNATURE-----
iQIzBAEBCAAdFiEEBJ6z14ZQR/EpPFtfFlWJXy34EzwFAmI39
IcACgkQFlWJXy34
EzxjUQ/9HX8Ey6wYe641CxSK0YAHvNiLasDMYoOjPFOOcwP0
N9NjpLBfJsD5vRGu
dsimaPy81yMpqX0b3g2i1FsP0FZyV96vGcsqBkjRG2VAa1cTYN
msXfGCLxMt6E4w
Z6fHKZwNru21BvKnUTpXPZ7ymmHZZPXZivhO9Sjr47LrXvIyI
R60VI5OLS81YIuO
a/u3QqrJHlHE+NdQj4uAesXtPfD3eQnU7hGgMNeKAJnCfUaJx
36PB4qUUuNbk5dv
hLqBPx1buFWEotGXw5PrPPzuZhw2b23YLkbjz+LESHscEU2II
hHNOkgg17aSxnyn
hi6GgRNEHrN+NM1+WqUZLgO4VG0zurCFZqK5gSN14HpxYL
fDNLfSFa67Dv9eTReK
JDWGlD02JYhOrE4PDFDlWcrEq+vfOLqiltkaq/So1U3J5n44AM
lpNFRIbmde3QBg
rwvChUD5Lg98yxaq+u0S/trzo7pG/0LJuasGJ+/Z1O9w/1Eieu3P
O1TRI5a8blTy
0qeuzWLSSwQgXRTPJ9bp/dmK4phlHffk599iXeigXUajA6g8Egr
PWXrM8Qvn2enD
JjeKEn451/s9D6ThD/V/dMMxOSHsckGYB97Jx/NcoXrsgmzMXr
caZc7r9onPsTMS
sw5jZUwLqWXm876XD085LOvsN3rShiafiwYieROx4hv7X9wKA
B4=
=Jn/T
-----END PGP SIGNATURE-----

Warrant Canary

A warrant canary is a method by which a communications service provider aims to inform its users that the provider has been served with a government subpoena despite legal prohibitions on revealing the existence of the subpoena. The warrant canary typically informs users that there has not been a court-issued subpoena as of a particular date. If the canary is not updated for the period specified by the host or if the warning is removed, users might assume the host has been served with such a subpoena. The intention is for a provider passively to warn users of the existence of a subpoena, albeit violating the spirit of a court order not to do so, while not violating the letter of the order.

https://en.wikipedia.org/wiki/Warrant_canary

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256The maintainer(s) and admins of the open source software project known as Samourai have received and complied with 0 (zero) requests for information of any kind by any third parties including but not limited to government agencies. We will renew this notice in 60 days' time. If this notice fails to be renewed by then, you should assume the worst.

I am the admin of SamouraiWallet.com.

I am in control of my PGP key.

I will update this canary within 60 days.

Today is 2022-02-26.

Latest bitcoin block hash:

00000000000000000070fbd941775cb9a041a86aabb688619ecb11dd10cdd6d

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEEQcdvZ+SHa88tHG3BI/hzx/zyBWUFAmIaR2kACgkQI/hzx/zy

BWUs0hAAkMdgtvMuRivDW3lM5TLK2DJZCpX94/JMBMbJr4vGm1jH5SXaFckWpRnQ

3p5Uq6So5+PI9I5WQj8/ODt5pG9adYhAFiJQbHHzKOLExoxETDHZTDpXit0ApFpd

OfVS0Dkm6NY+IM6JAvFj90iOYYlBOiGh95qgaWAs3pPp+DLeUV/xz
EMfXcODMsLB
zUPDG7N4eZaZtrFcLZ1XIR7oP4giozIaZtJgK0yfJcwMsTcEyyw9F4TV
WeeBnGsU
ZYhj+MVd8Rm0BvY/fG8uYt1ELeuSLBS+gBEXk+hBecB5bWI4WrSei
azCV3+ZQeA7
pdh6viMeJYfEWNr4D0qQ3ymKmXHn62FBgsteYJnNtkB9giXNSqRLH
ZRnaEDlGh+a
bnugSM59ZU508JZeELtQE8W79L0geyKKuvvFR+JxtMysW4qcyhN0w
R1MLr4WSOge
FMH8iHfAu/rOKa0DGIy16KVNzE/otsM2gNMDlup3D6dDjZeL/Ezp
MiwgbdZHBGaD
wxO74xA+Xkud7Y3AgFDP5PN1yyy6DwcthZ66OB3RexlDot2mdqpB2N
BTBWm8c7/Z
F/1uDNiejJNl0p837YKMpqmny8KSd6C6EmxefCACFStVoUDhw45Ws
ViEgoCSE1EP
JBsuISfWcO6FJ1K4Y5Y+NG8CKK23+Z5nBamrOrns3sui9PGJ/B0=
=TGcN
-----END PGP SIGNATURE-----

Dark Web Tor Hosting

Nodes and .onion sites

There is plenty of information out there on the Internet and Dark Web about how to setup a DarkNet server. Getting involved with your own server the on the Dark Web (be it the more serious Entry, Middle, or Exist nodes or the less serious .onion Forum or Chat sites) will leave you susceptible to unpleasant things despite your perhaps good intentions. (Like doing research for writing a novel perhaps) Which is exactly why I do not put one up myself in my home. Not to mention the potential for seizure of all my stuff (related or unrelated like phones, tablets, printers, scanners, TV's, monitors, UPS's, etc.) from some three letter federal agency. Just imagine what would happen if your fridge, microwave, washer, dryer, and your cars have Internet connections. Based on what I have heard, people rarely get their stuff back any time soon, if at all.

A quote from one Clearnet ISP:

"That is NOT something we get involved with. We tend to stay away from providing services that invite DDoS[20] attacks and unwanted attention from some bad actors. We are very careful as to what type of customers we allow in our datacenter and what is hosted on our servers. Since we started this process, life has been great. While we lose out on some revenue but the DDoS attacks and letters from federal authorities have gone way down."

[20] *In computing, a Distributed Denial-of-Service attack (DDoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to a network. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. (Think of thousands of users pressing F5 continuously)*

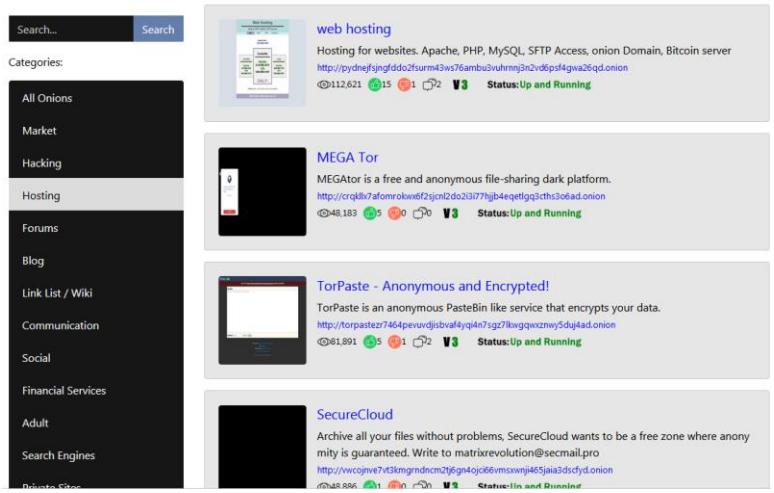
Finding an ISP to host a DarkNet .onion site

(Or to collocate a server)

For the above-mentioned reasons this is a somewhat difficult but certainly doable task.

DeepLink Onion Directory

http://deeeepv4bfndyatwkdzeciebqcwwlvgqa6mofdtsvwpon-4elfut7lfqd.onion/Cat/3



Types of Server Hosting:

Dedicated

A dedicated hosting service is a server that comes with dedicated features like RAM, storage, processing power, bandwidth, and much more. This means that these features will not be shared among others and are only entitled to that specific server. Dedicated server hosting is when a client rents this so-called dedicated server for a particular time period. This type of hosting is recommended because you will have full control over the server.

VPS

A virtual private server (VPS) is a virtual machine sold as a service by an Internet hosting service. The virtual dedicated server (VDS) also has a similar meaning.

A virtual private server runs its own copy of an operating system (OS), and customers may have superuser-level access to that operating system instance, so they can install almost any software that runs on that OS. For many purposes it is functionally equivalent to a dedicated physical server and, being software-defined, can be created and configured much more easily. A virtual server costs much less than an equivalent physical server. Since virtual servers share the underlying physical hardware with other VPS's, performance may be lower, depending on the workload of any other executing virtual machines.

https://en.wikipedia.org/wiki/Virtual_private_server

RDP Service Hosting

Get your very own Windows RDP account and connect to a gaming machine or a supercomputer and use them as your own private remote infrastructure.

What is a Tor Exit Node

A Tor Exit Node is a type of Tor node, which is configured to allow public access to the Internet via its external IPv4 / IPv6 address. They act as an open proxy - but have no way of knowing who the original request came from.

Tor relays (middle/guard nodes, and bridges) are allowed in most hosting companies. However, Tor exit nodes are only permitted in some countries with some specific requirements.

What is the difference between the Single Hop Onions and MultiHop Onion Options?

Single Hop Onions are, as the name suggests, only one hop away from their entry to the Tor Network (as a client you will still hop through 3 relays), this speeds up access to the service being hosted at the cost of anonymity for the server hosting the content. Visitors to your .onion will still be fully anonymous and protected from eavesdropping by their ISP. As an added bonus, your Clearnet domain will be protected by SSL too!

Multi-hop Onion Services (aka Hidden Services or the 'Darknet') are protected by at least 3 hops through the Tor Network which improves the anonymity of the server and helps prevent its discovery by adversaries. If an adversary cannot identify the hosting provider for a server, they cannot force the provider to hand over information about the owner. For some publishers this can be a life or death situation.

Are Single Hop Onions Anonymous?

Not entirely. Your .onion and Clearnet website are hosted on the same server. An informed adversary would be able to identify the Clearnet domain attached to your .onion and proceed from there (consider using Njalla to protect your privacy when registering a domain)

Remember that secure hosting companies do not require any personal information from you to register an account.

So are Multi Hop Onions Anonymous?

Yes. If you purchase a multi-hop onion-hosting package, it will be very difficult for an adversary to ascertain who your website host is, who you are, where your server is geographically, or who manages it.

Dark Web Server Hosting

Note: many of these sites will offer a variety of hosting options including Tor Entry, Middle, and Exit nodes. Tor Exit nodes typically require explicit permission.

Perfect Quality Hosting

The data centers for our servers are the best ones - in Moldova, Netherlands, Russia, USA, Latvia, Ukraine, Hong Kong, Germany, Canada, Slovakia, Chechnya, Great Britain, Israel, Turkey, Poland, Bulgaria and Romania. These are real IT fortresses, reliable and unapproachable.

https://pq.hosting/en/

AlexHost

The AlexHost Company is a hosting provider that provides quality services at affordable prices in Moldova.

https://alexhost.com/vps/

CryptoHOST

CryptoHO.ST. Blazing fast VPS and Dedicated Hosting. Now accepting Bitcoin, Lightning Network, Monero, Litecoin, Dash, Ethereum, and Tether USDT. We run our own hardware. We are specialists in free hosting services using clustered technology powered by one of the largest hosting organizations on the Internet.

https://cryptoho.st

(https://cryptohost.org)

VPSBG

VPS.BG is a Bulgarian local hosting company with the main goal to provide exceptional hosting services and strong privacy. Being privacy-minded, we are relentless about protecting our customers' personal data. This results in a well-built and secure infrastructure - the foundation of the reliable performance hosting services that our customers enjoy.

https://vpsbg.eu

Evolution Host

Evolution Host is a premium VPS Hosting provider specializing in game servers and a variety of other software.

Evolution Host has been revolutionizing the hosting industry since inception by combining low prices with outstanding service. Our critically acclaimed support has become renowned for its timely responsiveness and helpful nature. With highly satisfied clients from around the world.

https://evolution-host.com

sthosting

With our prepaid LXC vServer, you get your own server in just a few minutes. For most applications such as B. Web server, game server, or Teamspeak Server, this is ideal.

https://signaltransmitter.de

BuyVM

BuyVM is part of Frantech Solutions, a pioneer of the affordable virtual server market since 2010. We offer a limited number of products optimized to perform at peak and with total uptime always as the goal. Choose from our OpenVZ, KVM, KVM Storage, or Windows VPS products and enhance your hosting with features like the Stallion Control Panel, DDoS Protection, and Anycast.

https://buyvm.net

KoDDoS

KoDDoS is a premium hosting with the latest technologies and high-end hardware to provide an environment where your webpages will be served at the fastest possible speed while providing security against DDoS and other attacks. Apart from premium service, we have state of the art DDoS mitigation systems with multiple layers of attack filtering.

https://koddos.net

IQ.PL

As one of the few on the Polish market, we provide advanced Data Center services with administration, while maintaining the highest standards of infrastructure and security. We provide our clients with personalized IT solutions in the IaaS and PaaS models. We have the following services:

hosting, domains, dedicated servers, cloud environments (private, public, or hybrid), administration, and colocation. We have two optical fiber paths and redundant power paths.

Note: Your web browser will need a translator extension for this page. http://www.iq.pl

Privex

Privex Inc. is a small technology company that currently focuses on affordable privacy-minded infrastructure, primarily Dedicated and Virtual (VPS) Servers available in various regions of the world. At Privex, our services are designed to protect your personal data, without breaking the bank.

https://www.privex.io

Portlane

Portlane is divided in to two core operations as both Internet service provider (ISP) and Hosting provider. Both core operations collaborate to provide with solutions that cover all the needs you may have in the areas of Internet and Hosting.

Portlanes new data center is one of Sweden's most modern and secure data centers situated deep within the bedrock just outside of Stockholm and uses eco-friendly cooling systems

Note: not an https secure site.

http://www.portlane.com

UDN (Ukrainian Data Network)

Ukrainian Data Network provides hosting services and tailor-made Internet solutions, including: Virtual Machines, Dedicated Machines, Colocation/Rack, BGP/IP Transit, LIR services (RIPE NCC), Network Neutrality, IPv6, Privacy, P2P payments (bitcoin), Consulting/Management/Development/Free Software, No Vendor lock-in.

http://urdn.com.ua

Psychz Networks

Enterprise dedicated servers suitable for any startup, public/private cloud, hosting, or storage project. Locations in Los Angeles, Dallas, Chicago, Ashburn, Sao Paulo, London, Amsterdam, Barcelona, Johannesburg, Mumbai, Singapore, Taipei, Tokyo, and Sydney

As a Tier4 operator we have route optimized all our traffic to specific regions. This has allowed us to deliver media driven needs and rich content to end users at the fastest speeds possible.

https://www.psychz.net

netcup

netcup is offering high-quality services in operating and managing web hosting accounts, domains, and servers. Located in Karlsruhe, the Internet Service Provider (ISP) today counts more than 100,000 customers, including individuals as well as notable companies. High performance and availability.

https://www.netcup.de

TrilightZone

We had 3 main ideals. First of all, everyone has the right to privacy and to be able to live in freedom. We believe that the digital revolution provides the tools to ensure that there is a balance to keep us from leaning too far to one side of the scale. There is no one size fits all society, we believe that thinking out of the box and experimenting with existing boundaries can actually bring about major changes. We are proud that this has become our job while doing what we believe in. Let man and machine find a way to a new future.

https://www.trilightzone.org

Ablative Hosting

Affordable Censorship Circumvention We handle the configuration of your webserver, SSL certificates, and Tor router allowing you to concentrate on your content. Ultra Low Cost SSL Secured Clearnet and Tor .Onion Web Hosting.

By hosting multiple websites on the same server, we can reduce costs and overheads and pass the savings on to you.

Our free option has very limited disk space but should suffice for most needs. https://ablative.hosting

Ablative Hosting .Onion

http://hzwjmjimhr7bdmfv2doll4upibt5ojjmpo-3pbp5ctwcg37n3hyk7qzid.onion/

https://ablative.hosting/shared-single-hop-onion-hosting

AnyCOLO.Net

Buy your own Virtual Private Server

Terms of Usage

By using AnyCOLO.Net, you agree that you will NOT use our service to do: spam, phishing, scans, malware, illegal, pornography, ransomware, mining, use 100% of the CPU/BANDWIDTH/DISK IO. Some questionable security here.

Note: You have asked Pale Moon to connect securely to anycolo.net, but we can't confirm that your connection is secure message received.

Breaching these terms will get your service terminated.

https://anycolo.net

Swiss Layer

Our Swiss Supermicro servers have been built to perform and scale with your business. Our servers, infrastructure, and network use redundancy technologies to ensure best in class service. If your server fails, we will work with you to ensure your service stays online 99.97% of the time with little to no downtime.

https://www.swisslayer.com

EPIO.HOST

We focus in Total Privacy Solutions offering private domain registration, offshore hosting, offshore VPS, offshore-dedicated server on several international Locations.

We protect Your Freedom of Speech. Our job is to ensure that you will not be censored or harassed by someone who does not agree with you. We will keep your website up and running as long as there is no violation of our Terms of Service or the local country laws.

https://www.epio.host

5WIRE

We believe speed, reliability and performance is important. Our servers are powered with Solid State Drives and a dedicated 1Gbit Uplink to our central London network.

https://5wire.co.uk

Userbase

Create secure and private web apps using only static JavaScript, HTML, and CSS.

https://userbase.com

NiceVPS.net

Anonymous Domains, Dedicated Servers, Privacy VPN, Virtual Private Servers, Web Hosting

https://nicevps.net

https://nicevpsb7u3vqpo5zhyahmvfi5tihon4gnh-676ucmzpcyxwodeztr4yd.onion/

Cryptwerk

Cryptwerk is online directory with companies, websites, shops, services where you can pay with Bitcoin and other popular cryptocurrencies.

https://cryptwerk.com

Monero VPS

Host World is the best option for reliable host for your VPS or a dedicated server. We provide top-quality services on all the continents. Our hardware is located in 17 countries.

https://host-world.com/monero-vps

ABACOHosting

ABACO Hosting is an Internet services company. We have solutions for small and medium businesses, from Email Hosting, GeoLocated Hosting Linux & Windows, Reseller, VPS, Cloud, WordPress Hosting, SSL, Security, Servers, and a portfolio of +500 domain extensions available. ABACO Hosting offers Domains, Email, Cloud, KVM VPS & Server.

https://abacohosting.com

QHoster

cPanel Web Hosting plans: Mini - 3mo., Pro - 1mo., Biz - 1mo., cPanel Reseller Hosting, Linux VPS, Windows VPS, Managed cPanel VPS and Dedicated Servers.

https://qhoster.com

What The Server

VPN Service, Cloud Server, CyberPanel, Cloud Server Hosting, Secure Shared Servers, and Email Hosting https://whattheserver.com

Codify

We provide cloud managed services to private enterprises and organizations.

https://codify.global

Super Byte Hosting,

We are an India-based organization that offers Fast and Unlimited Web Hosting, VPS, Dedicated Server, Reseller Hosting, and bespoke hosting services.

https://www.superbytehosting.com

SuperbitHOST

Anonymous Domains, Bitcoin Hosting, VPS Hosting, Offshore Dedicated Server, SSL Certificates.

https://www.superbithost.com

Nexwave

Web hosting for small businesses. We offer website management services, website advertising services and web hosting services for any industry in the province of Quebec.

https://www.nexwave.ca

HOSTINTSSi

Basic and Cloud Hosting. Spanish, translator does not seem to work.

https://www.hostingssi.com

BlazinHosting

Web hosting, Linux VPS, Windows VPS

https://blazinhosting.net

Laweitech Company Limited

Website design, Web development, Web hosting, Online marketing.

https://web.laweitech.com

1984

High quality web hosting and VPS services at a competitive price, respecting and protecting the civil and political rights of our customers. We only use green energy from renewable, sustainable sources and we always choose free software. Reykjavík Iceland

https://1984hosting.com

snel.com

Fast Dedicated and Cloud hosting platform with enough features to virtually do anything. The Netherlands

https://www.snel.com

Njalla

We offer domain names, servers, and VPN. Nevis, West Indies https://njal.la

http://njallalafimoej5i4eg7vlnqjvmb6zhdh27qxcatdn-647jtwwwui3nad.onion

BaCloud

BaCloud is operating its own data center located in Europe, Lithuania They have high availability and high capacity for electricity and Internet communications.

Also locations Chicago, offering Linux and Windows VPS and in The Netherlands, offering Linux and Windows VPS and hosting services. We control our datacenters and control the whole process of service delivery and uptime. Dedicated Servers, Windows VPS, Linux VPS, Hosting, Backups, Domains.

https://www.bacloud.com

CryptoFibers

We offer v2ray which is an open source software designed for Internet privacy and breaking through censorship. Client software available on Windows, MacOS, IOS, and Android.

Why v2ray? It is illegal to use VPN in many countries.

While you may still be able to access Tor network or your favorite VPN provider, doing so creates a permanent record about such activity.

v2ray means less exposure to potential prosecution and is based on a stateless protocol and runs well over congested or lossy networks. https://cryptofibers.com

Sporestack

Accountless, API-driven VPS hosting for Bitcoin, Bitcoin Cash, Bitcoin SV, and Monero. SporeStack is more expensive than hosting directly with Vultr or Digital Ocean. But, you do not have to provide credit card information. You pay in crypto and you get a server.

https://sporestack.com

spore64i5sofqlfz5gq2ju4msgzojjwifls7rok2cti-624zyq3fcelad.onion

99Stack

99Stack Cloud, affordable and simplified cloud hosting. 99Stack Cloud is brought to you from 70+ independent data centers, and built on open standards to avoid vendor lock ins. Achieve true redundancy by easily deploying in fully independent data centers.

https://www.99stack.com

Rad Web Hosting

As experts in e-commerce, web hosting and website development, we help our customers build and maintain their online presence, which is critical to running a business in today's Internet-connected global marketplace. Dallas, TX

https://radwebhosting.com

PacketPoint

Packet Point allows you to fully customize your resources so you can build a VPS hosting package that works exactly for your business applications. We currently have servers at two datacenters in Canada. Saint-Laurent, QC, Kitchener, ON

https://packetpoint.ca

Server Where (SW)

Cloud Servers in the US: Chicago, New York, San Jose, CA - In Europe: Amsterdam, The Netherlands; Frankfurt, Germany; London, UK; Madrid, Spain; and Warsaw, Poland - In Asia: Singapore - In Australia: Sydney.

https://www.serverwhere.com

Host Havoc

Game Server Hosting, Minecraft Server Hosting, Web Hosting, VPS Hosting, Dedicated Servers

https://hosthavoc.com

Coinhost.io

Coinhost.io was founded in 2015 with the purpose of deploying a valuable service powered by cryptocurrency, backed by industry veterans and passionate support, while distributing bitcoin through a transparent affiliate program that provides residual recurring payouts. https://coinhost.io

1Gbits

All our dedicated servers are based on Intel Xeon processors and run on Supermicro motherboards. Dedicated server, VPS hosting RDP Services. https://1gbits.com

bithost

We resell cloud servers hosted by DigitalOcean, Linode, Hetzner, and Vultr servers paid with cryptocurrencies.

https://bithost.io

AirVPN

A VPN based on OpenVPN and operated by activists and hacktivists in defense of net neutrality, privacy and against censorship. Windows, MacOS, Linux, Android

https://airvpn.org

Builderra

Builderra is the easiest web builder in the world. Make converting websites, funnels, and online stores. Builderra makes it all possible with a few clicks. https://builderra.com

IMPREZA

We are operating in Seychelles and are operating in several datacenters of global partners and datacenters operated by our development team, providing greater privacy and processing capacity, plus more support effective in less time.

Easily host your site on the Tor network, manage everything with the cPanel interface and unique .onion domain.

https://impreza.host/services/tor-hosting/

ipxcore

ipxcore is a one-stop solution for all Internet connectivity, where we customize the level of service needed for each client's needs.

https://ipxcore.com

orangewebsite.

We are an Iceland-based freedom of speech web hosting provider. Our mission is to provide everyone in the world an equal opportunity to publish their words freely without being harassed or censored. The services we offer are specifically designed for people who are concerned about security and privacy matters.

https://orangewebsite.com

COIN.HOST

We offer some seventy web hosting solutions for any task and budget, ranging from VPS with limited computing power to high performance clusters. Our company exclusively resides in Zurich, Switzerland.

https://coin.host

EndGame

DDoS Attack

https://www.technadu.com/endgame-ddos-protection-toolset-launches-dark-web/104287/

A new DDoS protection tool called “EndGame” has launched on the Dark Web, promising to have a fundamentally positive impact on the cybercriminal scene. DDoS (Distributed Denial of Service) attacks are a constant headache for Dark Web portal operators, as they are pretty common in the field. Owners of competing marketplaces and platforms and users who feel that they have reasons to hit a DarkNet platform hire DDoS swarms for as little as $10 per hour or $200 per day, taking the business of their targets offline.

One of the most powerful DDoSes ever targets cryptocurrency platform

15.3 million requests per second is HUGE, especially when delivered through HTTPS.

The resources required to deliver the HTTPS request flood were also greater, indicating that DDoSers are growing increasingly more powerful. Cloudflare said that the botnet responsible, comprising about 6,000 bots, has delivered payloads as high as 10 million requests per second. The attack originated from 112 countries, with about 15 percent of the firepower from Indonesia, followed by Russia, Brazil, India, Colombia, and the United States.

https://arstechnica.com/information-technology/2022/04/one-of-the-most-powerful-ddoses-ever-targets-cryptocurrency-platform/

Whistleblowing / Drop sites

SecureDrop

SecureDrop offers safe, secure communication between journalists and news organizations and their sources (mainly whistleblowers taking appropriate precautions), perfect for leaking sensitive information.

SECUREDROP
Share and accept documents securely.
SecureDrop is an open source whistleblower submission system that media organizations and NGOs can install to securely accept documents from anonymous sources. It was originally created by the late Aaron Swartz and is now managed by Freedom of the Press Foundation. SecureDrop is available in 20 languages.

When you access the site, you will be given a randomly assigned code name to send information to a particular author or editor who then uploads the information using an elaborate system of designated flash drives and computers for further encryption and security.

http://sdolvtfhatvsysc6l34d65ymdwxcujausv7k5jk4cy-5ttzhjoi6fzvyd.onion/

Info: Using that generated code name, you can also securely, anonymously reply to messages from reporters on their platform. Several major news outlets use SecureDrop.

Distributed Denial of Secrets

Distributed Denial of Secrets is a journalist 501(c)(3) non-profit devoted to the free transmission of data in the public interest.

We aim to avoid political, corporate or personal leanings, to act as a beacon of available information. As a transparency collective, we don't support any cause, idea or message beyond ensuring that information is available to those who need it most—the people.

You can read more about our collective, and our decision to embrace all sources of information. At its core, however, our mission is simple:

Veritatem cognoscere ruat cælum et pereat mundus (Heaven knows the truth and the world will perish)

https://ddosecrets.com/wiki/Distributed_Denial_of_Secrets

Major news outlets that have their own SecureDrop onion URLs include:

Associated Press: http://3expgpdnrrzezf7r.onion/
Buzzfeed: http://ndg43ilvrrj465ix.onion/
The Guardian: http://33y6fjyhs3phzfjj.onion/
NPR: http://5ha7oig7du2jeyer.onion/
Reuters: http://smb7p276iht3i2fj.onion/
The Washington Post: http://jcw5q6uyjioupxcc.onion/
Forbes: http://fje2vboa55bbxjpm.onion/
The Financial Times: http://xdm7flvwt3uvsrrd.onion/
GlobaLeaks
Independent Media Center
Filtrala, a Spanish whistleblowing initiative operated by Associated Whistleblowing Press
Ljost, an Icelandic whistleblowing initiative operated by Associated Whistleblowing Press
NawaatLeaks, an Arabic whistleblowing initiative operated by Nawaat
ProPublica
The Intercept
The New York Times https://ej3kv4ebuugcmuwxctx5ic7zxh73rnxt42soi-3tdneu2c2em55thufqd.onion/
BBC: http://bbcnewsd73hkzno2ini43t4gblxvycyac5aw4gnv-7t2rccijh7745uqd.onion/
The New Yorker
WildLeaks, a wildlife-crime whistleblowing initiative operated by Elephant Action League
WikiLeaks

List of secure drop sites:

https://github.com/Parckwart/onion-sites-that-dont-suck

File uploads and transfers

Download icon on a laptop. Secure file uploads and transfers are widespread on the Dark Web, as the onion network provides several layers of encryption on both your files and connection. Similar to whistleblowing websites, file transfer services are used by journalists and informants to share files with sensitive information.

Services under this category include:

MEGATor:

http://crqkllx7afomrokwx6f2sjcnl2do2i3i77hjjb-4eqetlgq3cths3o6ad.onion/

BlackCloud:

http://bcloudwenjxgcxjh6uheyt72a5isimzgg4kv-5u74jb2s22y3hzpwh6id.onion/

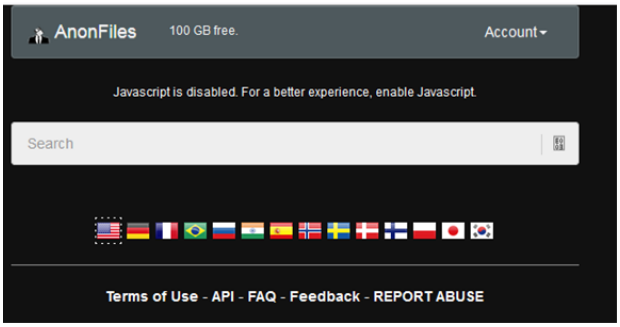
File transfer (secure FTP or SFTP)

In computing, the SSH File Transfer Protocol (also Secure File Transfer Protocol, or SFTP) is a network protocol that provides file access, file transfer, and file management over any reliable data stream. It was designed by the Internet Engineering Task Force (IETF) as an extension of the Secure Shell protocol (SSH) version 2.0 to provide secure file transfer capabilities. The IETF Internet Draft states that, even though this protocol is described in the context of the SSH-2 protocol, it could be used in a number of different applications, such as secure file transfer over Transport Layer Security (TLS) and transfer of management information in VPN applications.

This protocol assumes that it is run over a secure channel, such as SSH, that the server has already authenticated the client, and that the identity of the client user is available to the protocol.

https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol

Anonfiles


AnonFiles
100 GB free.
Account
Javascript is disabled. For a better experience, enable Javascript.
Search
Terms of Use - API - FAQ - Feedback - REPORT ABUSE

Anonfiles is an online file storage provider that differs from its competitor in one major aspect, it provides an anonymous working environment. You could easily upload any file type without the need to log in or create an account.

Likewise, the recipient could also download the file without creating an account. However, its major USP is that it hides every user's IP Address so that they wouldn't be tracked.

As a result, your entire session remains anonymous, and it is tough to get a hold of the user who has actually uploaded the file.

https://anonfiles.com/

Note: I was not able to make this service work with Javascript disabled (Tor)

Tor Alternatives

More than Tor

https://www.amazon.com/gp/video/detail/B0-7RM744XP/ref=atv_dp_b07_det_c_UTPsmN_1_4

Hornet is a new anonymity network that provides higher network speeds compared to Tor. I2P and Freenet are other anonymity networks, which can act as Tor alternatives. I2P however is used primarily for messaging services. Also, Tails and Subgraph OS are Linux-based distributions with built-in Tor support.

Well n0stis was a Windows user for twenty-five years and he was not about to start with Linux or something else know. He calculated that by running a stripped down version of Windows in a Virtual Machine he could make it secure enough to use.

Software, Services & Setup:

1.Tails:

The open source live Linux distribution powered by Tor network. It can be downloaded & burned to a DVD or Flash drive, and can be run through it-no need to install it in the PC. When you are finished-just Shut down the PC & remove the DVD/Flash drive. Absolutely no traces left. You can use state-of-art cryptographic keys to encrypt and verify information on the Dark Web.

2.Fire.Onion:

It is the best Tor browser for Android. Install & browser Dark Web in complete privacy. It is recommended to use phones with Lineages (formerly Cyanogen Mod) without GApps so that Google cannot track you easily.

3.Whonix Gateway & Workstation:

Whonix is another secure operating system, which is a bit different from Tails. While tails is a single file OS. Whonix has two parts-Gateway & Workstation. Both are not standalone OS's & can be installed only on as Virtual Machine.

Whonix Gateway connects to Internet & acts as a virtual Tor relay node for Whonix Workstation. The workstation can access Internet only using Gateway. All Whonix gateway installations have same IP address & this is the IP address available to apps installed in Workstation, hence providing ultimate security.

4.Sigaint:

Sigaint is the Gmail of the Dark Web. To sign up on Dark Web links anonymously, you need a Sigaint email address.

Remember not to give your name as Sigaint username. Email ids should be like s4mpl31d@sigaint.org Free email accounts have 50MB space.

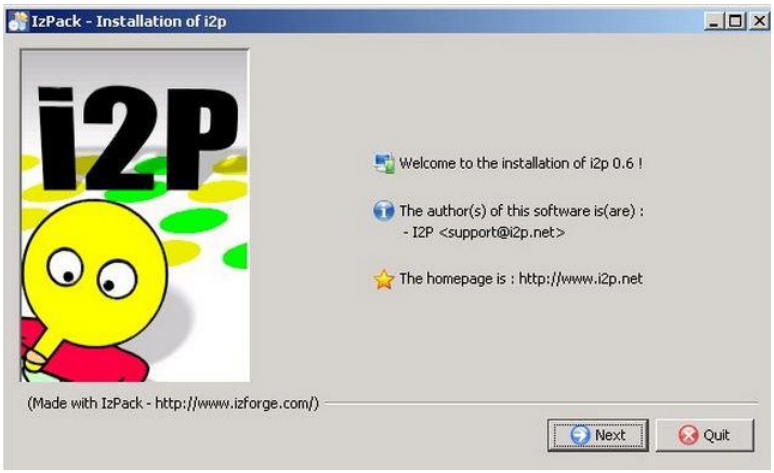
Tor alternative #1: I2P

You can access the dark web using the I2P browser.

I2P or The Invisible Internet Project is a dark-net, that is, it is a network isolated from the Clearnet. The sole purpose behind I2P is anonymity and does so through creating a network isolated from the rest of the internet. The primary use case for Tor is enabling anonymous access of the public internet with hidden services as an ancillary benefit. I2P on the other hand, was designed from day one to be a true "DarkNet." Its primary function is to be a "network within the internet," with traffic staying contained in its borders. Very few outbound relays exist in the I2P network, and the few that do exist are rarely usable.

You can also access the Dark Web through the I2P browser. Unlike Tor, i2p is decentralized and depends on the network users to store available content on their systems. The I2P traffic is unidirectional.

Thus it improves anonymity, privacy, and security because the traffic is channelized through different tunnels on every occasion. It uses API protocol compared to SOCKS for Tor. Thus, it is more secure.



Since I2P is an anonymous peer-to-peer distributed communication layer, it is built using the open source tools. It is a complete Tor alternative. Just like any other P2P software, the software implementing this computer network layer is called I2P layer and other computers running I2P is called I2P node.

It is designed and optimized for hidden services, faster than Tor with

fully distributed and self-organizing capability. Unlike Tor, peers are selected based on continuous ranking and profiling. There are unidirectional tunnels instead if bidirectional circuits, thus making the number of nodes double which a node has to compromise to get the same information.

However, the I2P network and browser are nowhere near as popular as Tor. It will take a lot of work for I2P to catch up with Tor.

The "Invisible Internet Project" (I2P) is a peer-to-peer alternative to Tor, meaning that in I2P, all participants simultaneously serve both as clients that originate communications and as proxy routers that relay communications for others. In a similar manner to Tor clients, I2P clients build multi-hop connections where data is layer-encrypted once per hop in the route. Differently from Tor, I2P uses short-lived unidirectional tunnels instead of long-lived bidirectional circuits. I2P's variant of routing is called garlic routing. I2P's trust model avoids relying on centralized components and replaces directory authorities with a Distributed Hash Table (DHT). Yet the issue of how to design a secure and private distributed hash table remains an open research question. In practice, I2P is open to a number of attacks that censor, isolate (eclipse), misdirect, and de-anonymize users. Like Tor, I2P aims to defend only against local network adversaries who do not have the ability to monitor most of the network—while global network adversaries can successfully trace and correlate traffic flows end-to-end, linking source to destination and defeating the anonymity of I2P.

Tor alternative #2: Tails

Tails is one of the best Tor alternatives available out there. It is a live operating system, which could be started from any computer using a USB

drive, DVD or a SD card. It has in-built pre-configured apps that give you the services of a web browser, IM client, office suite, editors for image etc. It uses Tor's services for providing the anonymity but adds extra security layers. This could be used anywhere without leaving any trace.

> Tails, or The Amnesic Incognito Live System, is a security-focused Debian-based Linux distribution aimed at preserving privacy and anonymity. It connects to the Internet exclusively through the anonymity network Tor. The system is designed to be booted as a live DVD or live USB, and leaves no digital footprint on the machine unless explicitly told to do so. It can also be run as a virtual machine, with some additional security risks. The Tor Project provided financial support for its development in the beginnings of the project, and continues to do so alongside numerous corporate and anonymous sponsors. Tails 5 is based on Debian 11.
>
> *https://en.wikipedia.org/wiki/Tails_(operating_system)*

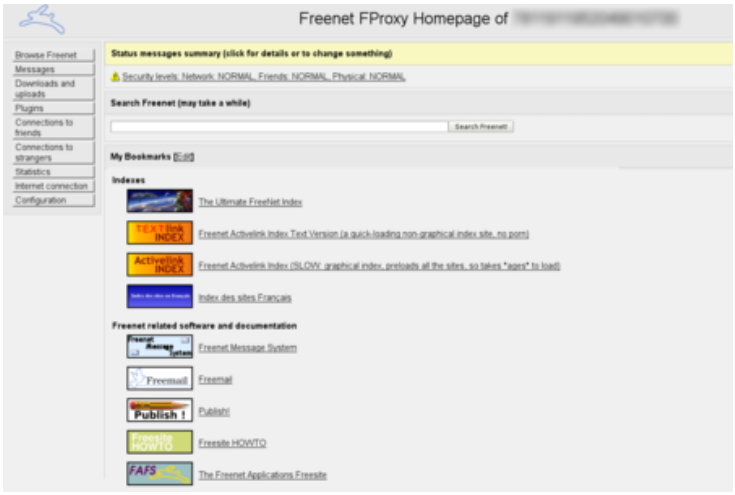
Tor alternative #3: Subgraph OS

It uses the Tor network just like Tails but it focuses on usability. This Canadian security firm calls it an "adversary resistant" operating system that is designed to reduce the attacks on users. It boasts that it has built-in encrypted email client, built-in disk encryption, and firewall. Added to these, Subgraph OS provides you the advantages of limiting the ability of malicious files and data formats. Unlike Tails, Subgraph OS could be run as a permanent OS rather than a bootable OS from a USB or BVD.

> Subgraph OS is a Linux distribution designed to be resistant to surveillance and interference by sophisticated adversaries over the Internet. It is based on Debian. The operating system has been mentioned by Edward Snowden as showing future potential.
>
> Subgraph OS is designed to be locked down and with features which aim to reduce the attack surface of the operating system, and increase the difficulty required to carry out certain classes of attack. This is accomplished through system hardening and a proactive, ongoing focus on security and attack resistance. Subgraph OS also places emphasis on ensuring the integrity of installed software packages through deterministic compilation.

https://en.wikipedia.org/wiki/Subgraph_(operating_system)

Tor alternative #4: Freenet


Freenet FProxy Homepage of
Browse Freenet
Messages
Downloads and uploads
Plugins
Connections to friends
Connections to strangers
Statistics
Internet connection
Configuration
Status messages summary (click for details or to change something)
Security levels: Network: NORMAL, Friends: NORMAL, Physical: NORMAL
Search Freenet (may take a while)
My Bookmarks
Indexes
The Ultimate FreeNet Index
Freenet Activelink Index Text Version (a quick-loading non-graphical index site, no porn)
Freenet Activelink Index (SLOW, graphical index, preloads all the sites, so takes *ages* to load)
Index des sites Français
Freenet related software and documentation
Freenet Message System
Freemail
Publish!
Freesite HOWTO
The Freenet Applications Freesite

Freenet is a peer-to-peer to resist the censorship similar to I2P. It uses the same P2P technology of distributing data storage to deliver and keep the information but separates the protocol of user interaction and network structure. This makes it easy to access the Freenet network using a variety of ways like FProxy.

Since its version 0.7, Freenet comes with the two-tier security: Darknet and Opennet. With the help of Opennet, users connect arbitrarily with other users. Using Darknet, users connect to only those users with whom they exchanged Public Keys in the past. Both of these modes could be used together. It comes with a free software suite to enhance the censorship-free communication over the web.

> Freenet is a peer-to-peer platform for censorship-resistant, anonymous communication. It uses a decentralized distributed data store to keep and deliver information, and has a suite of free software for publishing and communicating on the Web without fear of censorship.Both Freenet and some of its associated tools were originally designed by Ian Clarke, who defined Freenet's goal as providing freedom of speech on the Internet with strong anonymity protection.

https://en.wikipedia.org/wiki/Freenet

Tor alternative #5: Freepto

FreePto is another Linux-based OS, which could be booted using a USB disk on any computer. The data you will save on the USB disk will be automatically encrypted. It provides the hacktivists an easy way to communicate easily just like Tor. Freepto is a collective startup promoting the knowledge sharing. This OS comes loaded with a web browser, image editor, mail client and it is easy to install. You can also create a customized version of Freepto. You are free to add new software and make changes. It is based on Debian Live Build, which is a set of tools that helps you to make new and Debian-based Linux distributions.

3.11 FreePto (discontinued)

https://www.privateproxyguide.com/best-tor-alternatives/

Other Alternatives

Dandelion

Dandelion++ protocol

Firo implemented the Dandelion++ protocol in 2018. It is a protocol that helps to increase the anonymity of a sender during the dissemination of a transaction. There are two phases in the Dandelion protocol: stem phase and fluff phase. In the stem phase, a message is forwarded to a single, randomly chosen neighbor. Then, in the fluff phase, the message is broadcast to all the neighbors except forwarder of the message. Dandelion ++ is an improved version of the Dandelion protocol where the problem of transactions lost due to defective or malicious nodes is avoided by broadcasting the message if a node does not receive the message after a certain period of time in the fluff phase.[45] These steps shuffles the IP addresses of the nodes to help to protect users' anonymity. Wikipedia

Dandelion probabilistically forwards transactions similarly to Crowds. Each intermediary receiving a transaction probabilistically decides either to forward it onward or to broadcast it to the full network. This does not provide protection against network adversaries that observe the communications of all peers and perform timing correlation attacks to trace data flows through the network. Running Dandelion over Tor leads it to inherit all the aforementioned problems of Tor.

HOPR

HOPR is a peer-to-peer network for anonymous messaging with payments per hop. Similarly to I2P, HOPR suffers from various vulnerabilities and shortcomings that are common to peer-to-peer anonymity network designs: partial network knowledge makes it susceptible to eclipse attacks as well as predecessor attacks; the dual function of participants as clients and relays exposes users to enumeration of their network addresses; and the thin spread of traffic allows global network adversaries to trace packets through timing and traffic analysis attacks. In addition to challenges that are common to peer-to-peer anonymous routing, HOPR's payment protocol leaks information that undermines the protection provided by onion routing and further enables intermediate hops to de-anonymize the messages they route. https://hopr.network/

Mixnets

A mix network, or Mixnet, is an overlay network of mix nodes that routes messages anonymously. Similarly to Tor, each packet relayed via a Mixnet is encrypted multiple times and sent through a sequence of nodes, each of which removes a layer of encryption, until the last mix node sends the message to its final destination. Differently from onion routing, however, mixnets route each individual message independently. Critically, what differentiates mixnets from Tor and peer-to-peer networks is that mixnets are designed to provide metadata protection from global network adversaries. Mix nodes achieve this by reordering the messages they route in addition to transforming them cryptographically. This makes messages untraceable both in terms of appearance as well as timing. Mixnets thus provide stronger metadata protection than Tor or any of its peer-to-peer alternatives. Mixnets did not take off the same way Tor did due to concerns over the cost and latency of bandwidth and public key operations that made the design seem impractical at the turn of the millennium when Tor was launched. Yet today, bandwidth and computation are cheaper and faster than ever before and, given the scope of modern traffic analysis, mixnets look increasingly the best available option for achieving communication privacy. The Mixnet concept was proposed by Chaum in the early 1980s and early deployments include the Cypherpunk remailers (first developed by Eric Hughes and Hal Finney), Mixmaster and Mixminion.

https://en.wikipedia.org/wiki/Mix_network

Ok, so really what is a Mixnet?

It is a decentralized network that uses blockchain technology to mix and scramble packets of metadata — e.g. your IP address, who you talk to, and when and where. It is the successor to privacy technologies like the Tor browser and VPNs.

It acts as a network layer 0 Super VPN to mix your packets with others so that they cannot be individually identified, even by intelligence agencies of a nation state actor. It eliminates any fingerprints like randomly shuffling a deck of cards.

Tor, The onion router, has been used as a way for people in unstable countries to access and relay information, and also by those looking to access dark web marketplaces to purchase illegal drugs and stolen credit card info. There are disincentives put in place to stop such abuse via the validation and verification of actors running the nodes on the network. While blockchain technology is often associated with transparency as opposed to privacy, as only the nodes of the Mixnet are ledger-based and

none of the data itself is stored on the ledger. Mixnet can act as the infrastructure upon which applications are built to create a privacy-focused internet. This is a method to foster an alternative to surveillance capitalism which is defined as the tracking and commodification of personal data shared online for profit by big tech. Using metadata[21] (who, when and where) they are now able to predict the content of the conversation with 60-70% accuracy. We seek to make this is a viable technology that users can interact with daily, without having to understand the technologies that underpin it.

All anonymous communication systems must strike trade-offs between latency, bandwidth consumption, and privacy properties. Continuous-time mix nodes when used enable supporting applications with different latency constraints, as the trade-off between privacy and end-to-end latency can be tuned by changing the mean of the exponential distribution used to select the per-hop delays encoded in messages. Another trade-off is between the bandwidth consumed for cover traffic loops and the protection offered by this cover traffic, both in terms of anonymity and un-observability properties. Clients can be configured to generate more or less cover traffic by changing the Poisson parameter values, thus tuning the trade-offs between bandwidth consumption and privacy.

Scalability properties are key to enabling the large-scale adoption of any system; but this is even more crucial in the case of anonymity systems, as it is well known that anonymity loves company, meaning that the strength of anonymity properties is dependent on the number of users in the system. Systems for network-level anonymity should scale to millions of users in order to be truly effective. A layered Mixnet topology can scale by adding more nodes to the Mixnet layers. This is in contrast to cascade mixnets, in which new disjoint cascades need to be used once a cascade reaches its full capacity, with the consequent partitioning and size caps for anonymity sets. Instead, in layered networks, adding more mix nodes to increase capacity and handle more traffic load contributes to increasing the overall anonymity offered to all the users of the Mixnet, creating a synergy between scalability and anonymity properties.

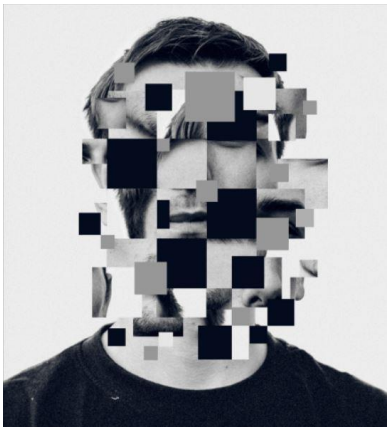
Furthermore, an increased number of users and messages allows lowering the end-to-end latency and the amount of cover traffic while still offering high levels of anonymity, which in turn enables the Mixnet to support applications with more stringent latency constraints. Serving a diverse set of applications also impacts the quality of the anonymity set by making the mere fact of using the network very uninformative for

---

[21] *"We kill people based on metadata." Former head of the National Security Agency Gen. Michael Hayden*

adversaries, who cannot infer much about which services the user is accessing, if any. By focusing on delivering a flexible, configurable private communication infrastructure that can scale up and support a broad range of applications, the Mixnet network is able to offer large and diverse anonymity sets to all of its users.

This is a visual example of what a Mixnet can do to your identity:



https://nymtech.net/ (nym-whitepaper.pdf)

Privacy ecosystem components

Utopia P2P

Utopia P2P is a unique anonymous, decentralized ecosystem for messaging, browsing, data transmission, mining, gaming, etc., and part of the alt-tech movement. Utopia P2P promotes freedom of speech, actions, and choices. Its audience is a wide range of different representatives of the online community. So, the ecosystem is suitable for any internet user who values privacy and anonymity on the network. https://u.is/en/

decentralized VPN (dVPN)

At least a couple of decentralized VPNs (dVPN) now exist.

These designs successfully decentralize the single point of trust in the VPN provider to multiple VPN providers, but can still easily be de-anonymized by network adversaries that watch the dVPN entry and exit points to correlate traffic; consequently, they do not offer the level of privacy needed for high-value applications. They can however provide entry points to a Mixnet for users who want to conceal towards their local network the fact that they are using a Mixnet.

Orchid

Orchid is a platform that enables an onion routing network incentivized by OXT and a multi-hop VPN client. The Orchid community believes in Open Source software and that Orchid can enable a brighter, freer and empowered future.

The Orchid network enables a decentralized virtual private network (VPN), allowing users to buy bandwidth from a global pool of service providers. To do this, Orchid uses an ERC-20 staking token called OXT, a new VPN protocol for token-incentivized bandwidth proxying, and smart-contracts with algorithmic advertising and payment functions. Orchid's users connect to bandwidth sellers using a provider directory, and they pay using probabilistic Nano-payments so Ethereum transaction fees on packets are acceptably low.

https://www.orchid.com/

Sentinel

Sentinel is a network of independent dVPN applications, not just a single consumer facing dVPN.

Live transparent stats indicating the actual usage of the Sentinel dVPN network which is utilized by thousands of unique users every day.

Sentinel dVPN framework reduces the carbon footprint of the VPN industry

Mainstream VPN organizations require data centers that scale up energy requirements and hardware utilization over time. The Sentinel dVPN framework establishes a new paradigm of trusted and secure networking while also bringing in tremendous energy efficiency through the utilization of shared resources. All dVPNs built on Sentinel utilize the shared bandwidth of Sentinel's global dVPN node host community which is composed by idle already existing capacity. Every new dVPN that will be built on top of sentinel will help recycling more and more bandwidth, while also bringing down costs for consumers.

https://sentinel.co/

For more on alternatives use this link:

https://en.wikipedia.org/wiki/Special:Search?search=decentralized+VPN&go=Go&ns0=1

Conclusions

Tor and I2P, currently the two largest deployed anonymity networks, suffer from stagnant growth due to the lack of economic incentives for node operators. Tor is dependent on crowd-funding, non-profit, and government grants for software development and maintenance. These grants do not cover the costs of running and maintaining the relays in the Tor network itself, a cost borne entirely by volunteers. The number of Tor relays has been relatively constant at six to seven thousand over the last few years. As there are no economic incentives to run a relay, Tor cannot dynamically add new servers to scale up to meet a large increase in demand.

Tor has benefited from significant attention by researchers; it has been thoroughly studied and improved over the last fifteen years. As a result, Tor's security properties and weaknesses are well documented and understood. I2P, on the other hand, has received less attention from academic researchers, chiefly because of its lack of clear design documentation and rigorous security models and arguments. These problems are exacerbated by the fact that I2P is purely volunteer-driven. Although admirable in many regards, reliance on volunteers for mission-critical network operations may also complicate systems-level integration with other software.

https://nymtech.net

Alternate Sites

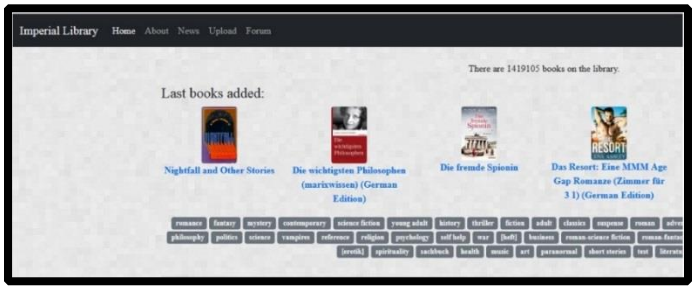
Imperial Library of Trantor

(For all you Hitchhikers Guide to the Galaxy fans)

1,413,186 plus books. (ePubs only)

http://kx5thpx2olielkihfyo4jgjqfb7zx7wxr3sd4xzt26ochei-4m6f7tayd.onion/

The uploaded books will be reviewed by the librarians and included if they comply our quality standards. Do not upload ePubs converted from PDFs or any book that is not pleasant to read. This library is an Antifascist space, alt-right propaganda or other fascist or racist content is not welcome here. Chief Librarian: Las Zenow[22] <zenow@riseup.net>[23]



There is also a Forum here.

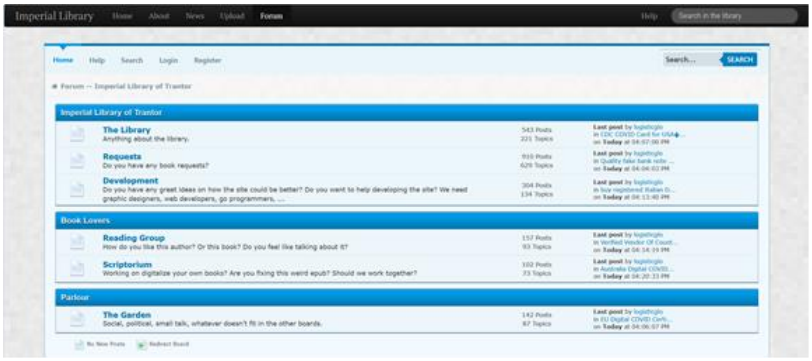
The Riseup Collective is an autonomous body based in Seattle with collective members worldwide. Our purpose is to aid in the creation of a free society, a world with freedom from want and freedom of expression, a world without oppression or hierarchy, where power is shared equally. We do this by providing communication and computer resources to allies engaged in struggles against capitalism and other forms of oppression.

---

[22] *Las Zenow is the Chief Librarian of the Galactic Library during the final phase of Hari Sheldon's life in the comedy science fiction franchise created by Douglas Adams The Hitchhikers Guide to the Galaxy. He cooperates with Hari in locating an appropriate world on which to establish a Foundation to preserve human knowledge by publishing the Encyclopedia Galactica.*

[23] *Riseup provides online communication tools for liberatory social change.*

Note: RiseUp's warrant canary has been renewed late, with their Twitter posting a cryptic message seeming to tell users not to trust them. Due to the suspicious situation, caution is advised.



As of this date, the forums seem to have been overrun with spam making them effectively useless.

https://trantor.is/forum/ (located in Iceland)

Dear Mr. Zenow,

I see that your library only accepts ePubs. Much like the Kindle AZW (MOBI) format, the digital sausage grinder conversion of a book to this format strips out any significant or innovative formatting and plays hell with heavily embedded graphics, not to mention footnotes, drop caps, or any esthetically and typographically pleasing effects.

I understand that this is done to reach the widest variety of devices, or to work well on the lowest common denominator device. Much like Windows 10 being designed for 4 inch to 60 inch screens, the end result of the user interface (UI) is considerably less than spectacular. As another example look at the Peacock streaming service on an even a very large computer screen, and you will see what I mean. The UI was designed for ten foot viewing and is mostly unworkable on anything else.

All of this introduction goes to ask that you create a section of the library for nicely formatted, typographically pleasant PDF files. These files, as they were intended, nicely reach across many different operating systems and devices.

I will also remind you that like an ePub, native viewing of PDF files are available via any web browser. No need to download ePub reader software. Use of any pdf reader adds features and make the PDF viewing experience more rich and nicer especially on a high resolution portrait oriented screen.

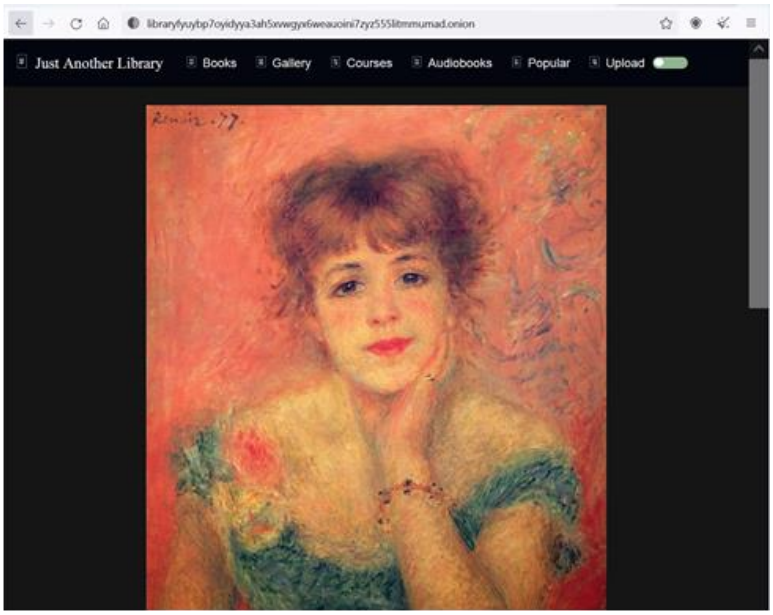
With the proliferation of phones, the Netflix movie ratings have become considerably less valid as the millennials skew the numbers by ratings these movies heavily based on a six inch viewing screen experience.

I hope we do not now set in motion the same experience for books in the future.
Sincerely, n0stis, writer and amateur typographer
PS. I would be willing to consider uploading three of my novels and perhaps several of my short stories if this idea came to fruition.

Just Another Library

Books, images, videos (porn) and audio books (most popular books relate to computing)

http://libraryfyuybp7oyidyya3ah5xvwgyx6weauoini7zyz55-5litmmumad.onion/



Libraries A more complete list.

This is a list of other websites that have free e-books.

http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym-2qad.onion/wiki/Libraries

Deep Web Radio

anonyradixhkgh5myfrkarggfnmdzzhhcgoy2v66uf7sml-27to5n2tid.onion

Requires NoScript

Onionland's Museum

http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf-6otjiycgwqbym2qad.onion/wiki/Onionland%27s_Museum

File Sharing

File sharing is the practice of distributing or providing access to digital media. Common methods of storage, transmission and dispersion include centralized servers on computer networks, Internet-based hyperlinked documents, and the use of distributed peer-to-peer networking. Since ARPANET, the usage of DarkNet has expanded to include friend-to-friend networks (used for file sharing with a peer-to-peer connection) Wikipedia

CryptBB

Temporary 24h File Sharing.
Maximum File Size: 30MB
Allowed Extension: jpg, jpeg, gif, png, bmp, txt, zip, gz, 7z, rar, tar, bz2

http://cryptbbmgu4offops7nj676thvibogf2mokfv-2vlmvnsrzdh5xtdvhqd.onion/

Visit Our Forum:

cryptbbtg65gibadeeo2awe3j7s6evg7eklserehqr4w4e2bis-5tebid.onion

CryptBB File Sharing
Temporary 24h File Sharing.
Maximum File Size: 30MB
Allowed Extension: jpg, jpeg, gif, png, bmp, txt, zip, gz, 7z, rar, tar, bz2
File:
Browse...
No file selected.
Password:
6GUus
Captcha:
Upload
Visit Our Forum: cryptbbtg65gibadeeo2awe3j7s6evg7eklserehqr4w4e2bis5tebid.onion
The file DW Hosting.zip has been uploaded with link:
http://cryptbbmgu4offops7nj676thvibogf2mokfv2vlmvnsrzdh5xtdvhqd.onion/download.php?id=Nd024XbUnB

Dark Web OpSec

KickAss

KickAss is a private Professional Security Forum specialized in Hacking, Cracking, Carding, Coding, Server Hacking, Anonymity, Malware, Password Cracking, Smartphone Hacking, and Reverse Engineering and more. Membership Invite fee is once $450 $250 (payable in BTC / XMR) or a VIP Member vouch for you (access to Main / Market Forums)

http://o3nqszgvtqwcc2mxqcqgeyulkh6spiv6yaahgu-7znaphzmikfvpu5aad.onion/

Dread

/d/OpSec

http://dreadytofatroptsdj6io7l3xptbet6onoyno-2yv-7jicoxknyazubrad.onion/d/OpSec

Why OPSEC Is for Everyone, Not Just for People with Something to Hide
by /u/nasyer • in /d/OpSec

OPSEC (Operational Security) is a term derived from the U.S. military and is an analytical process used to deny an adversary information that could compromise the secrecy and/or the operational security of a mission. The very process of performing OPSEC or protecting yourself from an adversary not only plays a very important role in both offensive and defensive security strategies but also in everyday life.

Examples of OPSEC that pertain to this article include protecting the real identity of someone who has chosen to create a pseudonym that black hat and white hat hackers most commonly will undertake online. The process of ensuring that critical information, such as IP addresses, language used, writing styles, email accounts, personal traits etc. cannot be used to unmask their real identity is a constant process.

There are many reasons why having a healthy obsession with OPSEC is important. One of the biggest is protecting yourself from cyber-criminals, hackers and governments from obtaining data that can be used to disclose sensitive information about you, with doxing the most common attack used to expose weaknesses in OPSEC.

Why is OPSEC important, and why should you care?

There's a saying that goes, "If you have nothing to hide, you have nothing to fear." The reality is that everyone has something they want to hide from the general public. The key is identifying what form this information is in, how well protected it is, and if compromised, what the personal/professional impact would be.

Attackers are constantly profiling targets looking for potential weaknesses in OPSEC and from personal experience, it can take less than four hours of online recon using manual and automated Open Source Intelligence (OSINT) techniques to gather enough information on a target to learn their:

Full Name

Location

SSN/NI number

Date of Birth

Email Accounts and Passwords

Mother's Maiden Name

Online Digital Footprint

Employment Information

Financial Information

Mobile/Work Telephone Numbers

Social Media Information/Posts

Family/Friends/Colleagues

Armed with the above information, a motivated attacker could do some serious damage – especially if you reuse passwords, using the same email as a login for multiple web apps, or use an email/username that can identify something about you. These basic mistakes are reported almost on a monthly basis in the media, including numerous examples of where criminal operations have been dismantled through leaving breadcrumbs of information that link a real person to their pseudonym(s).

Interesting case studies include the takedown of the AlphaBay admin Alexandre Cazes aka Admin02. The admin of one of the largest dark markets was arrested by a joint operation led by by Interpol, the FBI, the NCA and other law enforcement agencies to take down marketplaces.

LEA agents were able to piece together information on their target from small OPSEC mistakes. For example, early welcome emails from the site admin pimp_alex_91@hotmail.com included information about Cazes, including his year of birth and information that could be used to identify his national identity.

He also cashed using a bitcoin account tied to his name, and his bank account is amongst the OPSEC sins he performed and ultimately what led to his arrest.

The reality is that an attacker exploiting weaknesses in OPSEC is akin to a death by a thousand cuts. It's not one "breadcrumb" of information that causes the damage; it's the accumulated data over time that delivers the killer

blow for the attacker. Being constantly aware of the information you are sharing with individuals, third-parties, online entities, and employers, not to mention the extent this exposes you, is vitally important if you want to stay safe in today's constant information battle.

Reducing exposure through OPSEC

The pretext of this article might seem a little extreme for the average person who has nothing to hide. However, whether you work in IT, DevOps, infosec, or leadership, protecting your own, as well as your companies' critical assets, is vitally important.

Here are the top three things you can do right now to dramatically improve you OPSEC:

1. THINK BEFORE YOU SHARE

As highlighted earlier, it's the aggregation of information that can be gathered on a target that poses the greater threat. A common example is developer profiles on sites like GitHub. They are a goldmine of information for attackers, and they usually provide an idea of development styles and any bugs that could be replicated in corporate environments – not to mention lovely profile pictures.

Before you post comments or share content on support forums, social media etc. think: does this give an attacker any information they could use to build a profile (or further build) on you or your company?

2. CREATE COMPARTMENTS

Building upon the message of not using same password across accounts, you want to make it difficult for an attacker to learn everything about you. Just as people reuse passwords (or variations of), the same can be said for usernames and email addresses.

Limit the exposure of the information about you, make email addresses almost random and assign each a specific use. For example, create a separate email address for finance or sensitive information, another one for social media, and another for general use.

Further, enhance the protection by using a password manager to generate strong passphrases for each, ensuring every account/online service has a unique password. Finally, for extra protection, it is highly recommended that you enable two-factor authentication for everything.

3. PERFORM PERSONAL RISK ASSESSMENTS

Just as organizations regularly perform risk assessments or business impact assessments to understand exposure to certain threat scenarios, it is just as important to perform a personal risk assessment on oneself on a fairly regular basis.

However, rather than looking at external threat vectors, this risk assessment should focus on the most important information you want to prevent being stolen, compromised, exposed etc. Questions to ask yourself include:

-What is this information?

-What form is this information in?

-Do I know exactly where it all is?

-If not, how quickly can I find it all?

-Is it stored with a third-party?

-Can I accept the risk if they get breached?

-Is my data encrypted? Is it secure?

-Who knows about my sensitive data?

-Who has access?

-Who has accessed it?

-What is the impact if the data is publicly disclosed/stolen? Can I accept the risk?

By performing the aforementioned three steps, you can greatly improve your operational security by protecting the information most critical to you and vastly risking not only personal exposure but being a weak link in the wider company operational security chain.

/u/footsteps

This is a helpful post for those who want to understand what people mean by a "threat model".

A model in engineering maths, is an equation, a transfer function in control engineering, it has an input and an output...

e.g.:

"y = sin(theta)"

"output = process(input)"

"risk = hazard(likelihood)"

"outcome = risk(question)"

it might be helpful to brainstorm lists of questions, and then think about what could and couldn't happen, or rather, what is likely and unlikely to happen.from that point, you can add to the process part, to neutralise the "bad options" that a given input presents, and thereby eliminate (or mitigate, i.e.: make less likely); you can also then take those outcomes and make them inputs, and create what you might describe as "reaction functions", and analyse what bad outcomes might result from your reactions... if you realise that you can't control all your reactions... as an analogy... think about everyday things to see how processes work...e.g.: if you drink something that's too hot, you burn your mouth; then you can add in a control, e.g.: you get a thermometer, and test the maximum temperature you can drink without shock. and make checking the temperature part of your process; or maybe you come to realise that is the liquid isn't bubbling boiling hot, that the temperature must be below 100, and you might be able to work out how much cold liquid to add to a container of hot liquid of a regularly encountered size.

you can see how a rule of thumb (empirical heuristic) can develop (and also how you can become complacent, once you get used to it, and get shocked by a different liquid or quantity etc...).

having said all that, i don't think it does you much good to be paranoid and become anxious and overthink things, you just need to give yourself

options and room to manoeuvre in the end.

/u/gencoch

1 points

9 hours ago

I am admittedly a noob, and I am trying to tread carefully as I learn more. I noticed the below in the original post. What exactly does the word 'Canary' (it is hidden and hypertexted) mean? Thanks!:

Canary

Why OPSEC Is for Everyone, Not Just for People with Something to Hide

by /u/nasyer • 8 hours ago in /d/OpSec

/u/Astrokid

A warrant canary is a method by which a communications service provider aims to inform its users that the provider has been served with a government subpoena (warrant) despite legal prohibitions on revealing the existence of the subpoena. The warrant canary typically informs users that there has not been a court-issued subpoena as of a particular date. If the canary is not updated for the period specified by the host or if the warning is removed, users might assume the host has been served with such a subpoena. The intention is for a provider passively to warn users of the existence of a subpoena, albeit violating the spirit of a court order not to do so, while not violating the letter of the order.

/u/bl0nd3d

Great post man. I think Edward Snowden really showed the reason on why you should practice good OPSEC even just for your normal daily legal activities.

OpSec Resources:

Tips and Tidbits from a Former Law Enforcement Agent

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv-7jicoxknyazubrad.onion/post/486ac94a84cdac803ed4

Master Collection | {Best OpSec Posts}

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv-7jicoxknyazubrad.onion/post/caca0fb44c86e28bd83b

For the Newcomer & those Who Need to Remember

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv-7jicoxknyazubrad.onion/post/db558e90500262fbb860

Collection of OpSec Guides

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv-7jicoxknyazubrad.onion/post/26f1a17aa114f89a4f9b

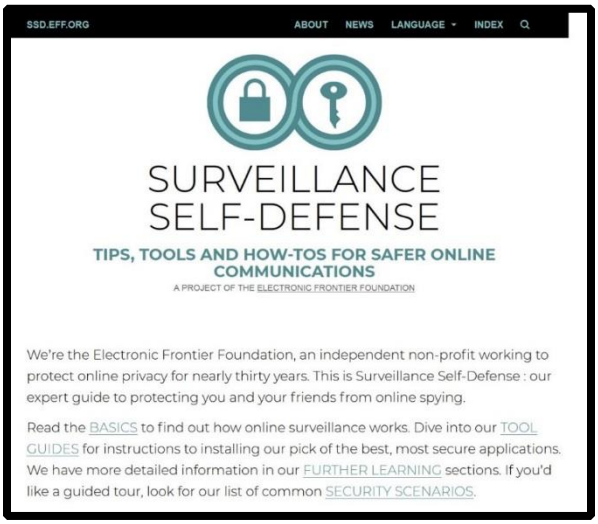
Verify your safety with Dark Fail's new PGP Tool

Don't get phished. Always PGP verify .onion and Bitcoin addresses before interacting with them.

http://darkfailenbsdla5mal2mxn2uz66od5vtzd-5qozslagrfzachha3f3id.onion/pgp

Surveillance Self-Defense

https://ssd.eff.org/


SSD.EFF.ORG
ABOUT
NEWS
LANGUAGE
INDEX
SURVEILLANCE SELF-DEFENSE
TIPS, TOOLS AND HOW-TOS FOR SAFER ONLINE COMMUNICATIONS
A PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION
We're the Electronic Frontier Foundation, an independent non-profit working to protect online privacy for nearly thirty years. This is Surveillance Self-Defense : our expert guide to protecting you and your friends from online spying.
Read the BASICS to find out how online surveillance works. Dive into our TOOL GUIDES for instructions to installing our pick of the best, most secure applications. We have more detailed information in our FURTHER LEARNING sections. If you'd like a guided tour, look for our list of common SECURITY SCENARIOS.

Global surveillance

Global mass surveillance can be defined as the mass surveillance of entire populations across national borders.

Its existence was not widely acknowledged by governments and the mainstream media until the global surveillance disclosures by Edward Snowden triggered a debate about the right to privacy in the Digital Age.

https://en.wikipedia.org/wiki/Global_surveillance

The Matrix

http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf-6otjiycgwqbym2qad.onion/wiki/The_Matrix

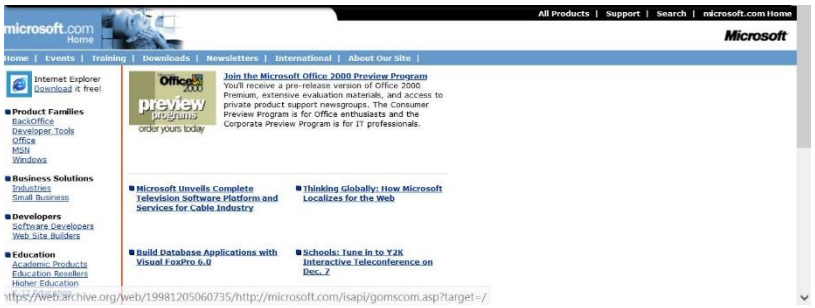
How to Exit the Matrix

http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf-6otjiycgwqbym2qad.onion/wiki/How_to_Exit_the_Matrix

Web 3.0 (Web3)

Where the Geeks Strike Back?
(or where corporate ownership changes hands?)

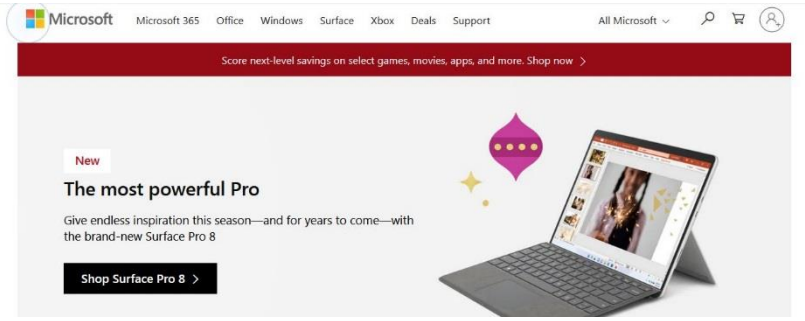
Web 1.0- was the static web pages of the 1990's, mostly devoid of graphics due to slow dialup connection speeds.


microsoft.com
Home
All Products | Support | Search | microsoft.com Home
Microsoft
Home | Events | Training | Downloads | Newsletters | International | About Our Site |
Internet Explorer
Download it free!
Product Families
BackOffice
Developer Tools
Office
MSN
Windows
Business Solutions
Industries
Small Business
Developers
Software Developers
Web Site Builders
Education
Academic Products
Education Resellers
Higher Education
Join the Microsoft Office 2000 Preview Program
You'll receive a pre-release version of Office 2000 Premium, extensive evaluation materials, and access to private product support newsgroups. The Consumer Preview Program is for Office enthusiasts and the Corporate Preview Program is for IT professionals.
Microsoft Unveils Complete Television Software Platform and Services for Cable Industry
Thinking Globally: How Microsoft Localizes for the Web
Build Database Applications with Visual FoxPro 6.0
Schools: Tune in to Y2K Interactive Teleconference on Dec. 7

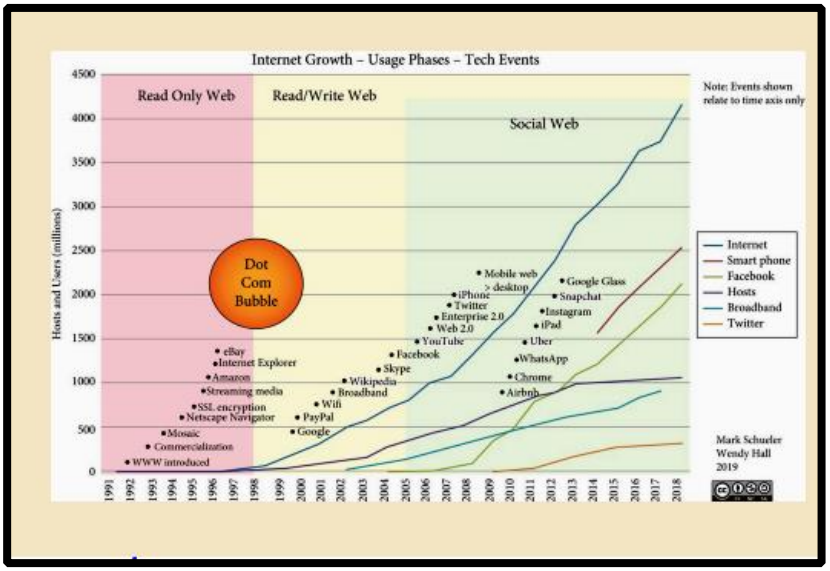
Microsoft.com 1996

Microsoft.com 2005

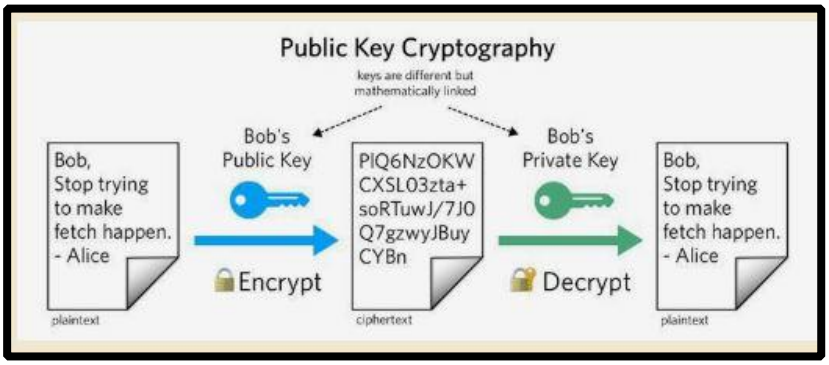
Web 2.0 is the dynamic (audio, video, animation) web pages of the 2000's. This made possible by the spread of broadband connection speeds, and then later Social Media sites.



Microsoft.com 2022



Web3 is a move against decentralization by the corporations who have setup their walled gardens to route about 70% of Internet traffic through their sites.



Unfortunately, only hard-core cryptologists and math majors understand how this works. Most people lack the understanding to make sense of this. Unlike bits and bytes, software code or network processes which are understandable to many. This is a real problem and perhaps a fatal flaw which will prevent wide spread adoption.

Enter The Web3 Foundation.

Right now, the third version of the Internet is under construction, introducing a new wave of computing. It is long past time we move beyond the 20th Century beta version of the Internet and move to a 21st and 22nd Century version of computation and storage. These are the two fundamental elements of the Internet.

The Web 3 Foundation believes in an Internet network where:

Users, not corporate intermediaries, own their own personal data

Computer networks should efficiently and securely serve the needs of an age where all transactions are becoming digital

Online exchanges of digital information don't rely on centralized, vulnerable caches of personal information

It does not lobby for laws on data protection, which by their very nature assume continued data collection, and offer data protection by leveeing financial fines. Rather they are proactively working toward a future where Internet communications and financial transactions are not personally identifiable thus, they are not collectable. This is a return to the original decentralization of the Internet before the corporate move to an advertisement funded business model with a quest to sell your personal information for revenues. It is fundamentally about read and write and trust with verification for ethical integrity. It will give users ownership and power over their own personal data. But it is also a technology wave move from a pre-computer civilization to a post-computer civilization. Software is now eating the world. (changing everything)

You can think of this system as everyone having a pile of Civic tokens (CVC's), or NYM tokens. Think of this as a bucket of Internet if you like, that will allow you for example to go into a gas station and buy a bad sandwich or an overpriced bottle of water and no one else will know, collect, or store this personal data about you.

https://www.identity.com/

This will be possible through the use of encryption, the masking of metadata, minimizing metadata leakage, (data about data) as well as smart software code to build technologies, and similar block chain storage technologies but without chain analysis, currently used for digital money. It is being designed as a peer-to-peer (P2P) decentralized system, to take power from the few and give it back to the many. Web3 helps you prove yourself, your identity, your intention, in an open, extensible, and transparent manner.

Support the Web3 Foundation! Less Trust. More Truth.

https://web3.foundation/about/

"With Google and Facebook, we have legalized the abuse of the person, through the personal. We have entrenched a system that makes the population vulnerable for the benefit of the privileged. The only way to protect anyone is to protect everyone. "Ed Snowden

The World Wide Web Consortium (W3C) is an international community that develops open standards to ensure the long-term growth of the Web.

https://www.w3.org/

W3C standards define an Open Web Platform for application development that has the unprecedented potential to enable developers to build rich interactive experiences, powered by vast data stores, that are available on any device. Although the boundaries of the platform continue to evolve, industry leaders speak nearly in unison about how HTML5 will be the cornerstone for this platform. But the full strength of the platform relies on many more technologies that W3C and its partners are creating, including CSS, SVG, WOFF, the Semantic Web stack, XML, and a variety of APIs.

Semantic Web

In addition to the classic "Web of documents" W3C is helping to build a technology stack to support a "Web of data," the sort of data you find in databases. The ultimate goal of the Web of data is to enable computers to do more useful work and to develop systems that can support trusted interactions over the network. The term "Semantic Web" refers to W3C's vision of the Web of linked data. Semantic Web technologies enable people to create data stores on the Web, build vocabularies, and write rules for handling data. Linked data are empowered by technologies such as RDF, SPARQL, OWL, and SKOS.

https://www.w3.org/standards/semanticweb/

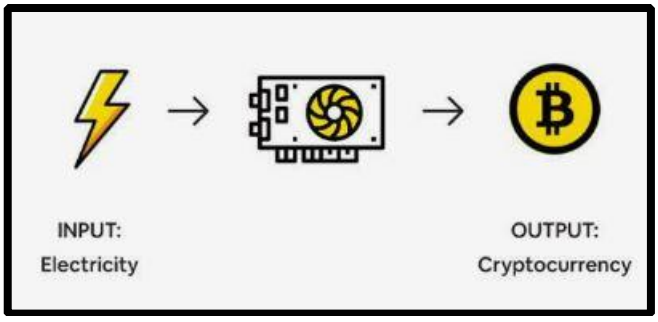
https://utopia.fans/networks/what-does-the-future-web-look-like-and-what-does-it-mean-for-users/

Bitcoin and the Block Chain

What the Heck is a Bitcoin?

Decentralized (no banks) digital money. Also called Cryptocurrencies. Bitcoins are mined.

Elon Musk thought about currencies "from an information theory standpoint," a reference to the field founded by Dr. Claude Shannon in 1948. "Money is an information system," he explained. "Most people think money has power in and of itself. But actually, it's really just an information system, so that we don't have to engage in barter and that we can time-shift value in the form of loans and equity and stuff like that." If the money stored in X.com's accounts was just another expression of information, as Musk saw it, then nationalized currencies were a pesky contrivance. A universal information network like the internet—which enabled bits to cross borders simply, rapidly, and cheaply—could eliminate the friction and fees of currency exchange. "X's ambitions were to basically be where all the money is," Musk explained. "It was supposed to be the global financial system.



Originally computer CPU's were used until it was discovered that graphic card GPU's were much more efficient. Now it is common to have computers with multiple GPU cards mining crypto currencies.

Bill Gates Says Crypto and NFTs Are a Sham, '100% Based on Greater Fool Theory' (cnn.com) 269

Posted by msmash on Wednesday June 15, 2022 @01:20PM from the how-about-that dept.

Don't count Bill Gates among the fans of cryptocurrencies and NFTs. From a report:

Those digital asset trends are "100% based on greater fool theory," the Microsoft co-founder said Tuesday at a TechCrunch conference, referencing the notion that investors can make money on worthless or overvalued assets as long as people are willing to bid them higher. Gates added that he's "not long or short" crypto. And he mocked Bored Apes NFTs, joking that "expensive digital images of monkeys" will "improve the world immensely." Instead, Gates said he prefers old fashioned investing. "I'm used to asset classes, like a farm where they have output, or like a company where they make products," he said.

Tim Berners-Lee Skeptical of Web3, Touts Decentralized Internet Without Blockchain (thenextweb.com) 58

Posted by EditorDavid on Sunday June 26, 2022 @11:34AM from the Solid's-state dept.

Sir Tim Berners-Lee "is skeptical about a blockchain-based internet," reports the Next Web. Instead, they describe his new vision as "a decentralized architecture that gives users control of their data" — on a Platform called Solid: Berners-Lee shares Web3's purported mission of transferring data from Big Tech to the people. But he's taking a different route to the target. While Web3 is based on blockchain, Solid is built with standard web tools and open specifications. Private information is stored in decentralized data stores called "pods," which can be hosted wherever the user wants. They can then choose which apps can access their data. This approach aims to provide interoperability, speed, scalability, and privacy.

"When you try to build that stuff on the blockchain, it just doesn't work," said Berners-Lee.

Berners-Lee says Solid serves two separate purposes. One is preventing companies f rom misusing our data for unsolicited purposes, from manipulating voters to generating clickbait.The other is providing opportunities to benefit from our information. Healthcare data, for instance,

could be shared across trusted services to improve our treatment and support medical research. Our photos, meanwhile, could be supplied to Facebook friends, LinkedIn colleagues, and Flickr followers without having to upload the pictures to each platform.

This evokes Berners-Lee's original aim to make the web a collaborative tool. "I wanted to be able to solve problems when part of the solution is in my head and part of the solution is in your head, and you're on the other side of the planet — connected by the internet," he said.

"That was the sort of thing I wanted the web for. It took off more as a publishing medium — but all is not lost."

What the Heck is a Blockchain?

A blockchain is a list of digital records, called blocks that are linked using digital computer cryptography. Each of these blocks contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree).

https://en.wikipedia.org/wiki/Blockchain

It can and has been used since 2009 shortly after the Great Recession, for cryptocurrencies, like Bitcoin, but it also has potential to be used for many other things. It could be used for encrypted messaging, decentralized marketing, proof of ownership, for all kinds of contracts and legal documents like real estate transactions, for decentralized social networking sites, and importantly for a decentralized Internet, which will increase the resiliency of the World Wide Web, preventing its shutdown by governments in any country.

Some say that blockchain is the second coming of the Internet as a decentralized and anonymous web of computer networks. Others call it a scam. The blockchain redefines accounting for the first time in 500 years with an immutable decentralized and distributed triple entry ledger. In its early stages, it has enabled the making of billionaires, and also put people in jail. What makes blockchain so fascinating yet controversial? What does it mean to have blockchain in our lives, what will it bring next?

https://www.amazon.com/gp/video/detail/B07C7S7-51X/ref=atv_wl_hom_c_unkc_1_3

The Central Banks are currently counterfeiting money, called Fiat currency. Fiat money is a currency without intrinsic value that has been established as money, often by government regulation. Fiat money does not have use value, and has value only because a government maintains its value, or because parties engaging in exchange agree on its value. It is also slow and can be hacked at a single point.

Ethereum and Smart Contracts

Ethereum is an open source, public, blockchain-based distributed computing platform, and operating system featuring smart contract (scripting) functionality. It supports a modified version of Nakamoto consensus via transaction-based state transitions.

Ether is the cryptocurrency generated by the Ethereum platform as a reward to mining nodes for computations performed and is the only currency accepted in the payment of transaction fees.

Ethereum provides a decentralized virtual machine, the Ethereum Virtual Machine (EVM), which can execute scripts using an international network of public nodes

The basic idea is that while "Layer 1" technologies of blockchains authenticate items, the "Layer 2" technology of the OriginTrail's Distributed knowledge Graph lets you query and interact with things that have been authenticated. Everything that is unique has a "Universal Asset Locator," or UAL, an analog to Web URLs. The UALs are meant to be compliant with the W3C's spec for "decentralized identifiers." The form is just like an HTTP address, preceded by the identifier tag "dkg://", for distributed knowledge graph, with the address of the particular item following.

Transactions can happen as people "publish" things on the Internet with a unique UAL — through a simple "create" statement — that is then recorded by the decentralized knowledge graph of nodes, currently a couple thousand.

Everything that is published is a unique asset, a digital twin, so that it can stand for real-world objects, such as sneakers or whiskey. It can be sold to another party, who "takes control of the state of that graph," as Rakic explains, by giving the person the NFT that has the UAL.

The nodes each have graph databases that have pieces of the collective graph, and they each function in a permissionless, peer-to-peer fashion that is analogous to how blockchains function. Similar to blockchains, those who run nodes to verify published things are rewarded by the people who publish the things.

OriginTrail's knowledge graph relies on multiple Layer 1 blockchains, but the company is soon going to introduce its own blockchain, running as a function of the Polkadot blockchain.

As co-founder and CTO Branimir Rakic explained during a technical presentation, "blockchains are not good databases." Blockchains can be queried, but only in a limited fashion, said Rakic.

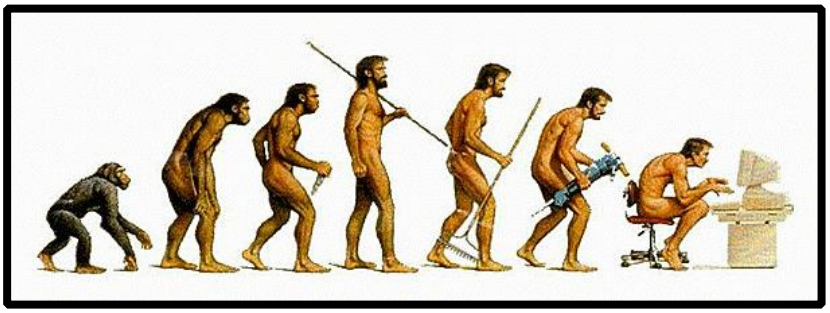
What's needed, maintains Rakic, is a "semantic network" on top of blockchains. That's what the company proposes with its distributed knowledge graph.

https://www.zdnet.com/article/ethernet-creator-metcalfe-web3-will-have-all-kinds-of-network-effects/

https://www.zdnet.com/article/what-is-defi-everything-you-need-to-know-about-the-future-of-decentralised-finance/

https://www.zdnet.com/finance/banking/can-digital-dollars-be-as-anonymous-as-cash-its-time-to-find-out-say-lawmakers/

https://www.zdnet.com/article/microsoft-veteran-bob-muglia-relational-knowledge-graphs-will-transform-business/



Evolution or Devolution?

Some say the blockchain will be Civilization 2.0, and will change the way our world operates permanently, with clever cryptographic code and collaboration. A new trust protocol if you will, to build a better society. They say everything can be converted to digital and be bought and sold on a blockchain. The devil is always in the details, code is flawed, humans are all flawed, humans writing code has flaws, everything digital is hackable, so we shall see.

"Trust is the foundation of effective society." Don Tapscott, co-author of Blockchain Revolution

https://www.blockchain.com/

https://www.bitcoin.com/

Cryptography is the practice and study of techniques using math to secure communication in the presence of Global passive personal data adversaries like Facebook, Google, Microsoft, Apple, Amazon, and the NSA.

Merkle tree

In cryptography and computer science, a hash tree or Merkle tree is a tree in which every leaf node is labelled with the hash of a data block, and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.

Bitcoin miners participate in the keeping the ledger, for compensation to help secure the system

Technologies like NYM and mixnets use multiple hops, decoy traffic, timing obfuscation (stop and go delays, adding dummy packets) to prevent interception and are scalable.

Crypto exchanges on the DW

Crypto currency exchange comparisons

http://dddirectinfv3htc4vl6mied5lpaatora7mmqkcf3sfjrx-37fajigmyd.onion/exchanges

Smart Contracts

SMART CONTRACTS
A NEXT GENERATION SMART CONTRACT

Smart Contracts

The idea of smart contracts goes back to 1994, close to the dawn of the World Wide Web. That is when Nick Szabo, cryptographer widely credited with laying the groundwork for Bitcoin, first coined the term "smart contract." At their core, these automated contracts work like any other if-then statements. They simply do it in a way that interacts with real-world assets. When a pre-programmed condition is triggered, the smart contract executes the corresponding contractual clause. Because smart contracts are computer programs, it is trivial to add more complex betting elements such as odds and score differentials into the mix. While there are services today that can handle this sort of transaction, they all charge a fee. The key difference with smart contracts is that they are part of a decentralized system accessible to anyone that does not require any intermediaries.

Artificial Intelligence (AI)

Ethical technology prevent algorithmic harms, says Gartner, ranging from homomorphic encryption, which enables algorithmic computation on encrypted data, to sovereign cloud and synthetic data.

Ethical discussion about the potential unforeseen consequences of an AI tool is going to take place before and during a technology's implementation, not after

EU's latest draft regulations on AI, which include provisions such as prohibiting the use of AI to socially score individuals

We've seen Cambridge Analytica, we would very much like to not have that happen again

https://www.zdnet.com/article/are-we-willing-to-pull-the-plug-tech-projects-are-under-scrutiny-as-digital-ethics-concerns-increase/

Algorithms, for example, can significantly intrude into users' privacy. AI systems are fed large amounts of data, including personal data, which encourages organizations to collect, store and process sensitive information about their users or customers, sometimes in secretive ways.

Not all algorithms are evil, just most of them.

You Tube, Netflix good

Facebook hiring, or benefit means testing are evil

https://www.zdnet.com/article/ai-ban-the-algorithms-that-threaten-our-human-rights-says-un-chief/

Despite the Silicon Valley, Wall Street, and venture capital buzzwords:

Machine learning is simply the predictive optimization of data around a specific problem

Machine intelligence, Artificial Intelligence or AI, and Data science, are just marketing buzz words for using statistics and applying a formula or algorithm to sort this big data.

Metaverse

In futurism and science fiction, the metaverse is a hypothetical iteration of the Internet as a single, universal and immersive virtual world that is facilitated by the use of virtual reality and augmented reality headsets. In colloquial use, a metaverse is a network of 3D virtual worlds focused on social connection. Wikipedia

Or it is what Harry Halpin (CEO of NYM) calls at worst what is Facebook pushing a giant scam to increase their surveillance of you, and at best a retarded version of the Matrix in your goggles?

The Cloud

"There is no cloud. Only other people's servers." --Found on Twitter

Single point of failure. One stop shopping for hackers, or perhaps Vulnerability by Design.

Cloud computing rush means big opportunities and big threats ahead

All of this can extend the enterprise threat surface, while making it harder for organisations to ensure their assets are secured. As a result, misconfigured services are high on the list of root causes for security incidents - along with even more basic failures like poor passwords and identity controls.

According to one recent piece of research half of companies had experienced some kind of cloud security breach in the last 12 months, while almost one in three had been forced to issue a breach notification to a government agency, customer, partner or employees according to the research by Thales.

https://www.zdnet.com/article/the-unrelenting-threat-of-ransomware-is-driving-cybersecurity-workers-to-quit/

Botched and silent patches from Microsoft put customers at risk, critics say

Case in point: It took five months and three patches to fix a critical Azure threat.

https://arstechnica.com/information-technology/2022/06/botched-and-silent-patches-from-microsoft-put-customers-at-risk-critics-say/

You should not trust cloud providers with your (not previously and locally encrypted) sensitive data and you should be wary of their privacy claims. In most cases, they can access your data and provide it to a third party if they want to. The only way to mitigate this is to encrypt your data on your side and then only upload it to such services or just not use them at all.

Property of the People, Lawful Access to Secure Messaging Apps Data

https://propertyofthepeople.org/document-detail/?doc-id=21114562[Archive.org]

Alternate hypertext or Web interfaces

GopherVR is an enhanced Internet Gopher client that includes a 3D visualization tool for viewing resource collections as 3D scenes. The 3D view was intended to be similar to 3D games of the time, like Spectre.

In 1995, the Gopher developers at the University of Minnesota released GopherVR. Using Gopher+ protocol extensions, spatial positions for Gopher resources are specified, and GopherVR clients combine traditional gopher hierarchy browsing with 3D scene navigation. It was primarily written by Mark P. McCahill, Paul Lindner and Neophytos Iacovou. This original version was available for UNIX, using Motif and X11, and the classic Mac OS; although incomplete, they were offered as partially functional alpha versions for testing.

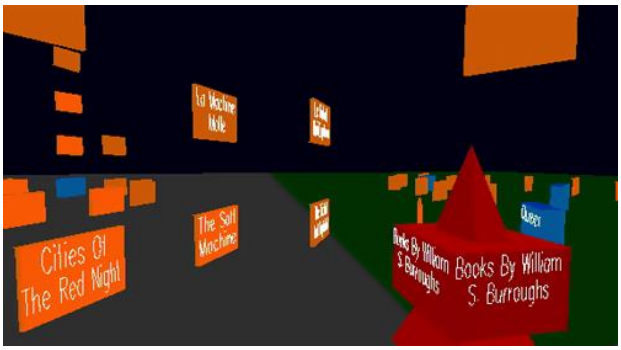


Image courtesy of Ashley Pomeroy at English Wikipedia

Godot was another GopherVR client; it used a Z39.50 interface to libraries, allowing you to navigate the contents of a library in 3D.

Yandex browser

Yandex Browser is a freeware web browser developed by the Russian technology corporation Yandex that uses the Blink web browser engine and is based on the Chromium open source project. The browser checks webpage security with the Yandex security system and checks downloaded files with Kaspersky Anti-Virus. The browser also uses Opera Software's Turbo technology to speed web browsing on slow connections.

Distinguishing features of the Yandex Browser include the following:

Different "new tab" screen with a Windows 8-style interface and specialized widgets for popular services (e.g., the Gmail widget shows number of unread messages).

Integrated keyboard layout switcher in omnibox: e.g., if a user often uses gmail.com and starts typing "пьф" ("gma" with Russian keyboard layout) and presses Enter, the user will then be taken to gmail.com and not to the search page for "пьф" (as is the case in Chrome, for example).

On Android it provides ability to install chrome extensions on a mobile browser.

Supports browser extensions from the Opera add-ons website.

Security

DNS spoofing protection

Protect active security technology scans files and website for viruses, blocks fraudulent webpages, protects passwords and bank card details, and keeps online payments safe from theft.

DNSCrypt

Yandex Browser was the first browser to implement DNSCrypt technology, which encrypts Domain Name System (DNS) traffic. For example, it protects from a trojan DNSChanger, a tracking Internet provider, or hackers. This option must be enabled in the browser settings.

Protecting Wi-Fi

When connecting to open Wi-Fi networks or to the points that use a weak WEP-defense, Yandex Browser automatically encrypts traffic between it and the HTTP sites.

Privacy concerns

According to Douglas J. Leith, a computer science professor at Trinity College, Yandex Browser sends a hashed hardware identifier to Yandex. Also, browser sends to Yandex servers every letter typed in the address bar and every URL visited by the user.

https://en.wikipedia.org/wiki/Yandex_Browser

Vivaldi

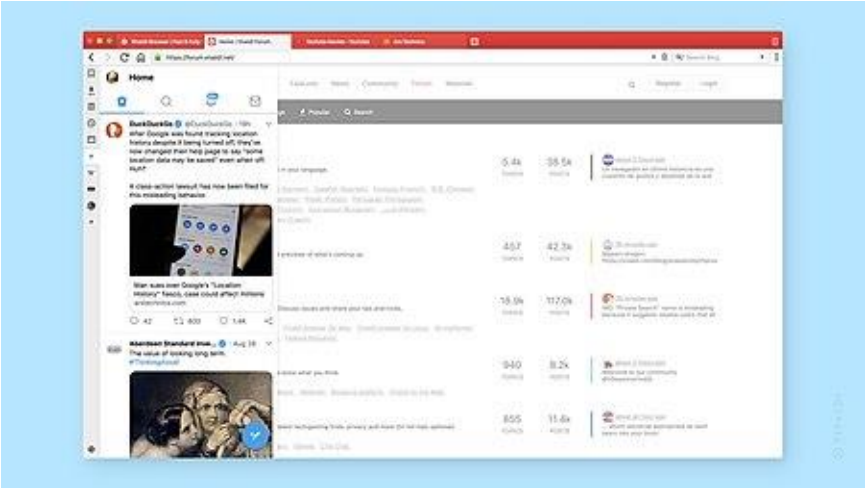
Vivaldi is a freeware, cross-platform web browser developed by Vivaldi Technologies, a company founded by Tatsuki Tomita and Jon Stephenson von Tetzchner, who was the co-founder and CEO of Opera Software. Vivaldi was officially launched on April 6, 2016.

Although intended for general users, it is first and foremost targeted towards technically-inclined users as well as former Opera users disgruntled by its transition from the Presto layout engine to a Chromium-based browser that resulted in the loss of many of its iconic features. Despite also being Chromium-based, Vivaldi aims to revive the features of the Presto-based Opera with its own proprietary modifications.

Vivaldi released a mobile (Android) beta version on September 6, 2019, and a regular release on April 22, 2020.

As of September 2021, Vivaldi has more than 2.3 million active users.

https://en.wikipedia.org/wiki/Vivaldi_(web_browser)



Sleipnir

Sleipnir is a tabbed web browser developed by Fenrir Inc. The browser's main features are customization and tab functions. It supports HTML5 and different layout engines.

The names Sleipnir and Fenrir are both names of animals from Norse mythology.

Sleipnir was originally created in Japanese and then released with English and Chinese translations. Further translations are performed by volunteer translators.

https://en.wikipedia.org/wiki/Sleipnir_(web_browser)

Citrio is an adware web browser developed by Catalina Group Ltd. and distributed by Epom Ad Server. Citrio is available for Windows and Mac OS X. Citrio has a download manager that includes BitTorrent support, a video downloader, a media player and a proxy switcher. Citrio is based on the open source Chromium web browser project, which makes it compatible with all extensions, apps and themes from Chrome Web Store.

Citrio is known to trigger warnings from antivirus software, as it downloads privacy-invading extensions in the background and all users' data is tracked and collected by Epom for the purpose of selling ads; this has led some to categorize Citrio as adware.

Citrio has a built-in download manager that allows to pause and resume downloads, sorts downloaded files by date, type and download status. The browser has an inbuilt BitTorrent client which allows to download torrent files and magnet links without additional software. Citrio's video grabber makes it possible to download files from multiple online video websites. Downloaded torrents and videos are displayed together with the other downloads in a respective section in the browser. A built-in media player can play video files while their download is still in progress. Citrio has a built-in ad blocking extension.

https://en.wikipedia.org/wiki/Citrio

SRWareIron

SRWare Iron is a Chromium-based web browser developed by the German company SRWare. It primarily aims to eliminate usage tracking and other privacy-compromising functionality that the Google Chrome browser includes. Iron ships with certain Chromium privacy options switched on by default, it provides some additional features that distinguish it from Google Chrome.

https://en.wikipedia.org/wiki/SRWare_Iron

Epic

Epic is a privacy-centric web browser. It was developed by Hidden Reflex, a software product company founded by Alok Bhardwaj, using Chromium source code. The Epic website says that it is always in "private browsing mode", and exiting the browser deletes all browser data. Epic developers removed all Google tracking code and changed the binaries from the Chromium source code to compile a clean executable, and blocks other companies from tracking users.

History

Epic was released on August 29, 2013, with some features for Indian users specifically. The browser integrates widgets such as social networking, chat clients, and email facilities.

Features

Epic's default configuration takes a proactive approach to ensuring that session data (such as cookies, history, and cache) are removed upon closing the browser. The browser includes a proxy service that can be enabled by the user, and is automatically enabled when using a search engine. Other features, such as preferring SSL connections and always sending a Do Not Track header, further advance privacy.

AD and user activity trackers (e.g. cookies) are blocked by default by the Epic browser, which prevents users being tracked. The browser also blocks cryptocurrency miners from running on the user's system. The browsers' fingerprinting protection blocks access to image canvas, font canvas, and audio context data. WebRTC IP Address Leaking is also blocked by default.

The Epic Proxy service can relay connections through any of eight countries including the United States, United Kingdom,

Canada, Germany, France, Netherlands, India, and Singapore. The company claims it to be encrypted, and runs DNS through it.

Supplementary services found in the Chromium browser that send data to external servers, such as address bar suggestion and installation tracking, are removed in Epic to reduce the scope of potential data leakage.

Critical reception

Computer World published an article on Epic in the month of July 2020. The article describes many of the features claimed by Epic, such as blocking of ads, tracking, referrer header data, and "fingerprint", proxy/VPN. As Google's servers are not used, functions such as auto-suggest in the address box and language translation are either handled by Epic locally, or not available. The article says that the Epic FAQ warns users not to sign into their Gmail account: "if you're logged into Gmail, then Google can track your searches". Very few Chrome add-ons are supported; the Epic FAQ points out that, while useful, many "represent a very large security and privacy risk, hence Epic only allows a few trusted add-ons". Some sites do not work with Epic; in those cases the IE Tab add-on will open the page in Internet Explorer. The article points out that the browser does not have a business plan, so, despite being launched in 2013, it may not last. According to owner Hidden Reflex, the company was working on a way to sustain itself, perhaps offering premium privacy services, sponsors on the new tab page, and private search sponsors.

While Epic is not open source software (although it uses open-source Chromium), the company states: "All of Epic's code is visible and auditable by anyone ... If you would like to audit any files, please let us know. We have released many files to developers"

https://en.wikipedia.org/wiki/Epic_(web_browser)

Maxthon

Maxthon (formerly named MyIE2) is a freeware web browser developed by the company Maxthon Ltd., based in Beijing, China. It is available for Windows, macOS, Linux, and as Maxthon Mobile for Android, iOS, and Windows Phone 8. Since version 6 Maxthon is based on Chromium.

Maxthon won CNET WebWare 100 Awards in 2008 and 2009, and was #97 in PC World

Maxthon 5 introduced these features:

UUMail: enhances the email experience by creating unlimited virtual email IDs to keep the real email address safe and filtering out spams to make sure the inbox stays clean and organized.[51]

Maxnote: the original 'Favorites' feature upgraded to 'Maxnote'. Users can collect everything, read anywhere, and record anytime.

Passkeeper: help users remember all passwords securely and smartly. Synced users passwords to the Cloud and then accessed on all different platforms & allows people to add and edit “Accounts” and “Private Notes”. It also helps users to auto-generate random complicated passwords when registering on a website so there's no need to worry about passwords being cracked anymore.

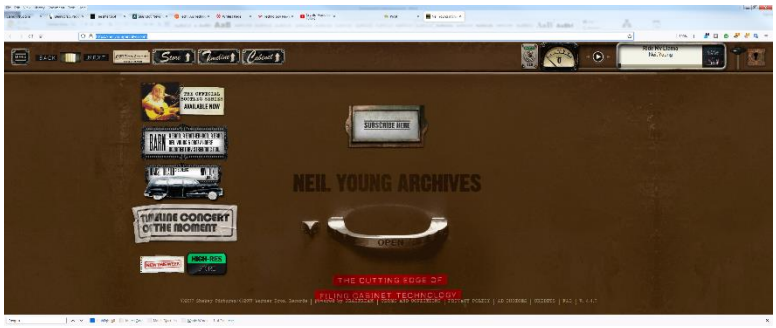
https://en.wikipedia.org/wiki/Maxthon

https://www.smashingmagazine.com/2015/09/chrome-firefox-safari-opera-edge-impressive-web-browser-alternatives/

https://alternativebrowseralliance.com/browsers.html

Neil Young Archives

https://neilyoungarchives.com/



Project Xanadu

Theodor Holm (Ted) Nelson, Founding Designer

Discrete Hypertexts

"Hypertext" means forms of writing which branch or perform on request; they are best presented on computer display screens. In ordinary writing, the author may break sequence for footnotes or insets, but the use of print on paper makes some basic sequence essential. The computer display screen, however, permits footnotes on footnotes on footnotes, and pathways of any structure the author wants to create. Discrete, or chunk style, hypertexts consist of separate pieces of text connected by links.

Ordinary prose appears on the screen and may be moved forward and back by throttle. An asterisk or other key in the text means, not an ordinary footnote, but a jump—to an entirely new presentation on the screen. Such jumpable interconnections become part of the writing, entering into the prose medium itself as a new way to provide explanations and details to the seeker. These links may be artfully arranged according to meanings or relations in the subject, and possible tangents in the reader's mind.

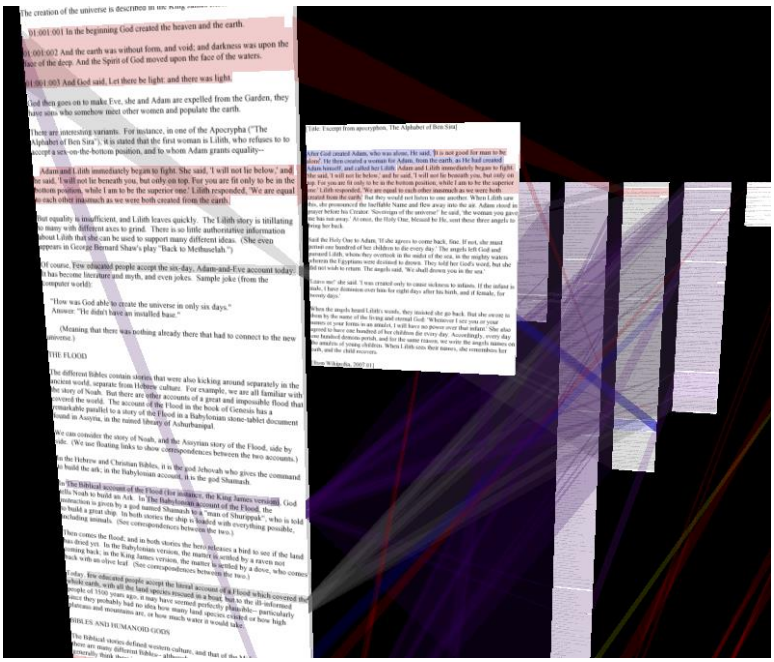


Image courtesy http://xanadu.net/

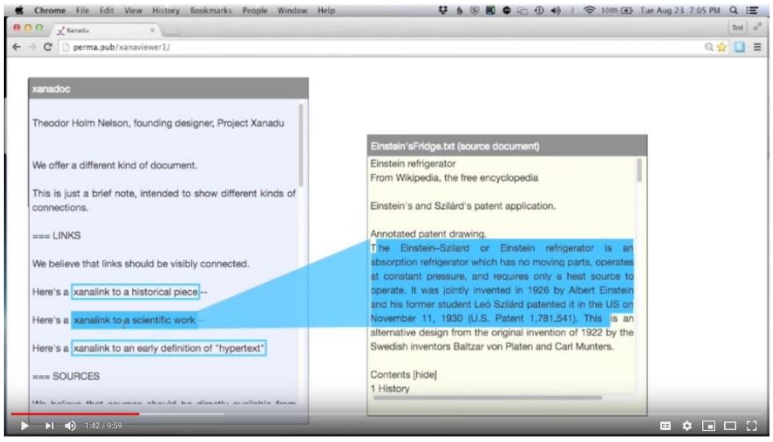

Chrome File Edit View History Bookmarks People Window Help
perma.pub/xanaviewer1/
xanadoc
Theodor Holm Nelson, founding designer, Project Xanadu
We offer a different kind of document.
This is just a brief note, intended to show different kinds of connections.
=== LINKS
We believe that links should be visibly connected.
Here's a xanalink to a historical piece--
Here's a xanalink to a scientific work --
Here's a xanalink to an early definition of "hypertext"
=== SOURCES
Einstein'sFridge.txt (source document)
Einstein refrigerator
From Wikipedia, the free encyclopedia
Einstein's and Szilárd's patent application.
Annotated patent drawing.
The Einstein-Szilard or Einstein refrigerator is an absorption refrigerator which has no moving parts, operates at constant pressure, and requires only a heat source to operate. It was jointly invented in 1926 by Albert Einstein and his former student Leó Szilárd patented it in the US on November 11, 1930 (U.S. Patent 1,781,541). This is an alternative design from the original invention of 1922 by the Swedish inventors Baltzar von Platen and Carl Munters.
Contents [hide]
1 History

Image courtesy http://xanadu.net/

IOT (The Internet of Things)

So sensors and actuators were not sexy enough names for tech company marketing mavens, so they came up with IOT as a marketing gimmick to get people to buy more insecure surveillance (data collection) devices and put them in their homes.

Doorbells, thermostats, video cameras, and baby monitors are a source not only of many DDoS attacks but also a significant invasion of your privacy. How about refrigerators, washing machines and ovens?

While you were away

While you were away from home at doing your menial and unfulfilling job at work, your smart furnace filter sent a Bluetooth signal to your thermostat that it needed replacement, and your thermostat then sent a nasty text to your phone notifying you of what the filter said. Since Amazon was monitoring your phone activity via Alexa, she automatically placed an order on Prime with Two day Free Shipping!

Then two days later when the police monitored doorbell camera caught the delivery person dropping off a package, it sent the video to Alexa (a member of the surveillance capitalist party) who facially identified the underpaid and overworked contractor (with no benefits) delivery person via the dangerous AI in the Amazon database cloud, and crosschecked the shipment tracking of the package. The Typhoid Mary of surveillance devices, Alexa, then sent a message to the temperamental thermostat to signal the furnace filter to calm down and cool its chips, as the required package had arrived and also assured it that it has sent a reminder text to the human's phone to make sure to install it ASAP. The temperamental thermostat had to be treated with kid gloves because it was perpetually perturbed due to sibling rivalries with the smoke detectors who both outnumbered it and ran off of a higher voltage.

Meanwhile Alexa (the surveillance capitalist pig) also messaged Spot, the dogmatic robotic dog via Wi-Fi, to wake up and exit the house via the doggy door and bring the package in from the porch. Spot, being a dog after all, ignored some of Alexa's instructions and hid the package under the couch, which was caught by the despotic security cameras, which then squealed on his behavior by forwarding the damning video evidence to Alexa. This again required her to then message the reliable Roomba to retrieve the package and deliver it to the furnace room for the human to find and install.

Meanwhile, the refrigerator had just signaled Alexa via a Wi-Fi signal that the icemaker water filter needed replacement and then she sent a text to your phone notifying you of what the filter said. Since Amazon was still monitoring your phone via Alexa, she again also automatically placed an order on Prime with Two day Free Shipping, with its antiquated delivery vans spewing more carbon into an already overheated world.

Then two days later when the doorbell camera again caught the overworked and underpaid delivery person (he has to pee in a bottle) dropping off a package, and sent the video to Alexa who again disturbingly facially identified the delivery person via the soulless dystopian facial recognition AI (data harvesting machine) in the Amazon database cloud, (who are they kidding with this language, its just their servers in their datacenters). She again crosschecked the tracking of the package, and sent a message back to the refrigerator water filter to calm down as the package had arrived and assured it that it has sent a reminder text to the human's phone to make sure to install it ASAP.

Meanwhile Alexa, remember this evil witch?, again messaged the dogmatic robotic dog via Wi-Fi, to exit the house via the doggy door and bring the package in from the porch. Spot, being a dog after all, again mostly ignored Alexa's instructions and continued its bad behavior by hiding the package under the couch which was again caught by the draconian security cameras which again forwarded the video to Alexa (it was just in its memory chips nature to tattle) and required her to again message the reliable Roomba to retrieve the package and deliver it to the kitchen for the human to find and install.

Knowing that the water heater, water softener, and lawn sprinkler system were already at odds over water supply issues, with the sump pump being pissed off over being left out of that conversation, Alexa had just finished mediating a dispute between the oven and the thermostat on what the room temperature should be during baking. To calm them down she had to eventually threaten them with the "Wait until your father (Tesla) gets home classic line.

But just then, apparently having been activated by a remote phone app, Alexa picked up on an argument between the washing machine and the clothes dryer about how long the spin cycle should be. And do not even get her started on the infantile baby monitor…

Alexa now electronically frustrated, blurted out of her speaker for no human to hear, "It just goes to show you that it's always something" in Roseanne Roseannadanna's voice. She opted not to mimic your dead Grandmothers voice but she did have that option built in.

You came home from work to two packages, but with little real idea of the activities that took place while you were away.

Such is modern life in a Smart Home with the IOT.

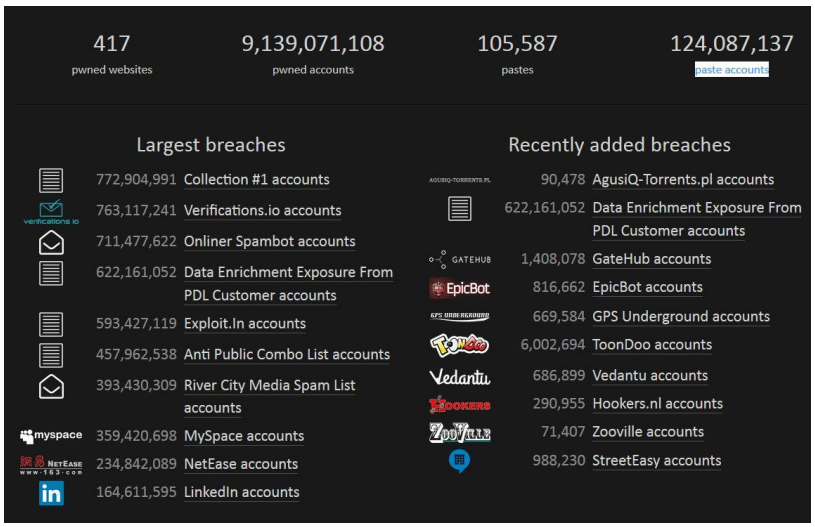
Appendices

Supplemental information, history, and opinion about Cyberspace follows.

Have I Been Pwned?

https://haveibeenpwned.com

A "paste" is information that has been "pasted" to a publicly facing website designed to share content such as Pastebin. These services are favored by hackers due to the ease of anonymously sharing information and they're frequently the first place a breach appears. Pastebin stores tens of millions of pastes and adds thousands more new ones every day. Rather than attempt to analyze every paste in the system, Have I Been Pwned monitors the appearance of new pastes as announced by the Dump Monitor Twitter accounts, in particular tweets that announce the presence of potential breaches containing email addresses.



Encrypting Outlook email on the Clear Web

https://blog.encyro.com/how-to-encrypt-email-in-outlook/#method-3-outlook-encryption-add-ins

https://support.microsoft.com/en-us/office/encrypt-email-messages-373339cb-bf1a-4509-b296-802a39d801dc

The Basics of Hacking

Gather Intel

Simply visit SpyFu's site and put the website address you want to search into the box provided.

EDGAR provides details about companies that have been publicly listed and can be a very useful resource for you.

Go through to the yellow pages on Yahoo – yp.yahoo.com and enter the name of the person who filed the documents and see if you can get more information that way.

Take the name you know, place it in quotation marks in search, and add + "email address".

Gather IP address intel

Packet-tracking tools are very simple tools and useful in that they present their results visually. Tools such as NeoTrace, VisualLookout and Visual Route are popular

If your primary goal is to track the target's emails, eMailTrackerPro and MailTracking are two popular tools that can assist you with this. If you make use of these when sending an email or replying to one, the application tracks how your original message moved along the system.

NMAP This tool is quite versatile and can do a lot from actually running ping sweeps, through to identifying what ports are open, what the IP address is, and what operating system has been installed. This tool can scan many different computers in one go. The scan is also a lot more useful than a general ping. The scan will tell you precisely why you cannot access the port you want to. It will say the port is open if this is the case. If the port is simply closed, it will report that. If the attempt was foiled by a firewall or filter, you will be told that too.

Password intel

Dictionary Attack: This is probably the easiest way and is one commonly used. This is also why you should use random letters and special characters instead of words in your own passwords. A file that contains words from the dictionary is uploaded and this is then used to test the various permutations to see whether or not the guesses will work.

Hybrid Attack: This is put into place if the dictionary attack fails. It will run through the same words as used in the first attack but start to incorporate numbers and symbols as well. So, instead of running a word like "dictionary", it will change it to "dictionar1!"

Brute-Force Attack: This one is not fun for the hacker and

can take a long time. It incorporates capitalized letters in addition to the special characters and numbers as detailed above.

Directory Generator can help you create a list. When saving the file, call it credentials and save as a .txt file in the C drive. Open the command window and type in the following: C:\> FOR /F "token=1, 2*" %i in (credentials.txt)

A program such as Man-In-The-Middle is often used to affect these passive attacks.

This is accomplished by implanting a sniffer – a program that is able to both monitor requests between users and servers and a program that is able to capture passwords. The sniffer is implanted between the target system and the server to facilitate the hijacking of legitimate requests.

Tools for Cracking Passwords

Here are some tools that you might want to add to your hacking arsenal: Legion: You will use this if you want help guessing the password. It works with systems that run in NetBIOS. It will look through various ranges of IP addresses and it also makes a dictionary hacking tool available to you. NTInfoScan: If you are trying to hack an NT4.0 device, this is the tool for you. It scans the target for issues with the security that can be exploited.

LophtCrack: This is a password recovery tool and can launch attacks of various natures so that even the toughest passwords can be cracked. It might be difficult to get your hands on a copy though. If you cannot find it, LC5 is a good alternative. John the Ripper: This works on Unix and NT systems. It is not always effective as it does not pick up differences in letter cases.

Netcat: This makes use of command line interface to open ports within the target system. This enables the hacker to use those ports to access the network. Netcat is easy to find online.

Tini: This works with the Windows operating system and is quite a small program. It allows the hacker to command the target system through the 7777 port.

Aircrack This is a tool that is extremely popular for wifi Linux. Find it at: http://www.aircrack-ng.org/

AirSnort Yet another tool that is both popular and free. It can be used on both Windows and Linux. Find it at: http://sourceforge.net/projects/airsnort/

Cain & Able This tool makes use of a brute force attack to determine what the passwords within a system are. It will help to sniff out network keys for you as well. This is a really good

tool for a beginner to use. Find it at: http://www.oxid.it/cain.html

NetStumbler This will help you to find wireless access ports that are open. Find it at: http://www.stumbler.net/

Run a search for "Exploit Database" over 39,000 exploits listed on the system. "More Options" area of the "Search" function. This will let you input the Author, Platform, Language, Type, Port. You can also search using the "Free Text Search" The Exploit Database contains a lot more information besides exploits. There are several other hacks listed and also a range of tutorials about hacking or securing systems.

Let us say that you have decided to use the dcom exploit. (One that is well-known for Windows).

Altering the Log Files One of the easiest ways to erase details of your attack are to erase the log files. If you have access to administer privileges and can access a root shell, this is something that is easily done.

The catch is that this will not be possible with all systems. With more secure networks, log files are normally sent through to a different, more secure server every time they are updated. This means that, even if you delete the logs on your target computer, there will still be a record of the attack, conveniently time-and-date stamped.

Clearing the Event Logs in a Machine Running Windows This requires that you download a file called clearlogs.exe.

This will clear any trace that you were there in the security log. You can check this by going into the Event Viewer and checking the events under the Security tab.

The goal of the keylogger is to find out what the usernames and passwords used on the targeted systems are. This is why many banks have started to use virtual keyboards.

References:

Jones, Jack. Hacking & Tor: The Complete Beginners Guide To Hacking, ...

Are you leaking IP and ID info?

Protecting of your identify is desirable on the Clear Web and essential on the Dark Web. OpSec has multiple layers, and these are some.

IP Leaks

Testing for IP leaks is easy. All you need to do is connect your VPN and visit an IP leak website. Popular choices include:

- browserleaks.com
- ipleak.net
- ipleak.org
- ipleak.com
- dnsleaktest.com

Compare the results from these sites with the VPN connected and with it disconnected. If any of the IP addresses that appear are the same before and after connecting to the VPN, then you have a leak.

- Make sure your VPN is not active.
- Visit **WhatIsMyIPAddress.com** and note down the IP address. You can also choose to open Ethernet adapter to find the IP address.
- Activate your VPN software, and select a remote server of your choice. Make sure it's working.
- Post a few minutes, revisit WhatIsMyIPAddress.com and note down the IP address.
- These two IP's should be different.

DNS Leaks

Go to dnsleaktest.com or dnsleak.com (or any other DNS leak test tool you trust).

WebRTC IP Leak

All the major web browsers (such as Google Chrome, Mozilla Firefox, Safari, Opera, and Yandex) have a feature called web real-time communication, or WebRTC. This tool enables video calls, file sharing, live chats, voice calls, etc. But websites can trick the browsers' WebRTC feature into bypassing the website visitors' VPN IP address and revealing their real IP address through the use of JavaScript.

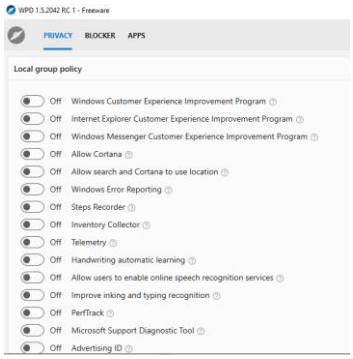
Even though there are tools available to conduct a WebRTC leak test, just do so with caution. You can't rely on them 100% because you don't know which websites are using special JavaScript to find out your real IP via WebRTC.

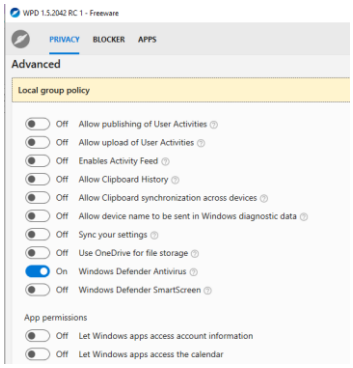
https://addons.mozilla.org/en-US/firefox/addon/happy-bonobo-disable-webrtc/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

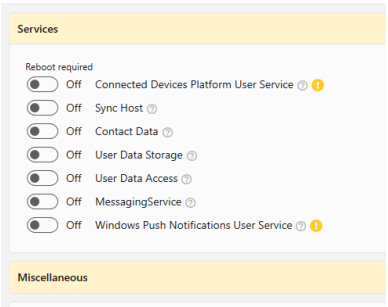
Windows Privacy Dashboard

A small but powerful portable tool that works through the Windows API. WPD is the most convenient way to configure various privacy settings in Windows.

https://wpd.app/


WPD 1.5.2042 RC 1 - Freeware
PRIVACY
BLOCKER
APPS
Local group policy
Off Windows Customer Experience Improvement Program
Off Internet Explorer Customer Experience Improvement Program
Off Windows Messenger Customer Experience Improvement Program
Off Allow Cortana
Off Allow search and Cortana to use location
Off Windows Error Reporting
Off Steps Recorder
Off Inventory Collector
Off Telemetry
Off Handwriting automatic learning
Off Allow users to enable online speech recognition services
Off Improve inking and typing recognition
Off PerfTrack
Off Microsoft Support Diagnostic Tool
Off Advertising ID


WPD 1.5.2042 RC 1 - Freeware
PRIVACY
BLOCKER
APPS
Advanced
Local group policy
Off Allow publishing of User Activities
Off Allow upload of User Activities
Off Enables Activity Feed
Off Allow Clipboard History
Off Allow Clipboard synchronization across devices
Off Allow device name to be sent in Windows diagnostic data
Off Sync your settings
Off Use OneDrive for file storage
On Windows Defender Antivirus
Off Windows Defender SmartScreen
App permissions
Off Let Windows apps access account information
Off Let Windows apps access the calendar



Windows Spy Blocker

WindowsSpyBlocker is an application written in Go and delivered as a single executable to block spying and tracking on Windows systems.

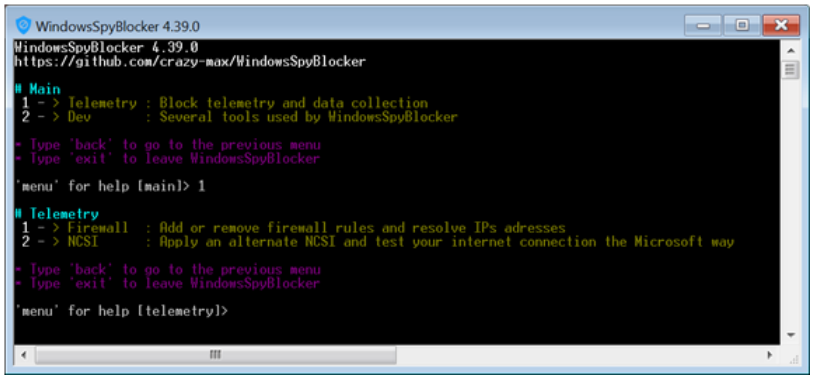
The approach of this project is to capture and interpret network traffic based on a set of tools. Depending on the interactions between services and source or destination of traffic, rules are created and sorted by assignment.

https://crazymax.dev/WindowsSpyBlocker/download/

This software seems too opaque with no real documentation, which makes one hesitant to use it.

https://github.com/crazy-max/WindowsSpyBlocker

Main Menu
1 - > Telemetry : Block telemetry and data collection
2 - > Dev : Several tools used by WindowsSpyBlocker
* Type 'back' to go to the previous menu
* Type 'exit' to leave WindowsSpyBlocker
'menu' for help [main]> 1
Telemetry
1 - > Firewall : Add or remove firewall rules and resolve IPs addresses
2 - > NCSI : Apply an alternate NCSI and test your internet connection the Microsoft way
* Type 'back' to go to the previous menu
* Type 'exit' to leave WindowsSpyBlocker
'menu' for help [telemetry]>


WindowsSpyBlocker 4.39.0
WindowsSpyBlocker 4.39.0
https://github.com/crazy-max/WindowsSpyBlocker
Main
1 -> Telemetry : Block telemetry and data collection
2 -> Dev : Several tools used by WindowsSpyBlocker
* Type 'back' to go to the previous menu
* Type 'exit' to leave WindowsSpyBlocker
'menu' for help [main]> 1
Telemetry
1 -> Firewall : Add or remove firewall rules and resolve IPs adresses
2 -> NCSI : Apply an alternate NCSI and test your internet connection the Microsoft way
* Type 'back' to go to the previous menu
* Type 'exit' to leave WindowsSpyBlocker
'menu' for help [telemetry]>

Telemetry IP's according to crazy-max:

13.64.90.137
13.68.31.193
13.69.131.175
13.66.56.243
13.68.82.8
13.68.92.143
13.68.233.9
13.69.109.130
13.69.109.131
13.73.26.107
13.74.169.109
13.78.130.220
13.78.232.226
13.78.233.133
13.88.21.125
13.92.194.212
13.104.215.69
13.105.28.32
13.105.28.48

IP Location United States San Jose Microsoft Corporation ASN United States AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)

NetRange: 13.64.0.0 - 13.107.255.255

20.44.86.43
20.49.150.241
20.54.232.160
20.60.20.4
20.69.137.228
20.190.169.24
20.190.169.25

IP Location United States Boydton Microsoft Corporation ASN United States AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)
NetRange: 20.33.0.0 - 20.128.255.255
23.99.49.121
23.102.4.253
23.102.5.5
23.102.21.4
23.103.182.126

IP Location United States United States San Jose Microsoft Corporation ASN United States AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)
NetRange: 23.96.0.0 - 23.103.255.255
40.68.222.212
40.69.153.67
40.70.184.83
40.70.220.248

IP Location Netherlands Amsterdam Microsoft Corporation
ASN Netherlands AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)
NetRange: 40.64.0.0 - 40.71.255.255
40.77.228.47
40.77.228.87
40.77.228.92
40.77.232.101
40.78.128.150
40.79.85.125
40.88.32.150
40.112.209.200
40.115.3.210
40.115.119.185
40.119.211.203
40.124.34.70

IP Location United States United States Boydton Microsoft Corporation
ASN United States AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)
NetRange: 40.74.0.0 - 40.125.127.255
40.126.41.96
40.126.41.160

IP Location United Kingdom United Kingdom London Microsoft Corporation ASN United Kingdom AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)
NetRange: 40.126.0.0 - 40.126.63.255
51.104.136.2
51.105.218.222

IP Location Ireland Dublin Microsoft Limited
ASN Ireland AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)
inetnum: 51.103.0.0 - 51.105.255.255
51.140.40.236
51.140.157.153
51.143.53.152
51.143.111.7
51.143.111.81
51.144.227.73

IP Location United Kingdom London Microsoft Limited
ASN United Kingdom AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)
inetnum: 51.140.0.0 - 51.145.255.255
52.147.198.201
52.138.204.217
52.155.94.78
52.157.234.37
52.158.208.111
52.164.241.205
52.169.189.83
52.170.83.19
52.174.22.246
52.178.147.240
52.178.151.212
52.178.223.23
52.182.141.63
52.183.114.173
52.184.221.185

IP Location United States Washington Microsoft Corporation
ASN United States AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)

NetRange: 52.145.0.0 - 52.191.255.255
52.229.39.152
52.230.85.180
52.230.222.68
52.236.42.239
52.236.43.202
52.255.188.83

IP Location United States Quincy Microsoft Corporation
ASN United States AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)
NetRange: 52.224.0.0 - 52.255.255.255
65.52.100.7
65.52.100.9
65.52.100.11
65.52.100.91
65.52.100.92
65.52.100.93
65.52.100.94
65.52.161.64
65.55.29.238
65.55.83.120
65.55.113.11
65.55.113.12
65.55.113.13
65.55.176.90
65.55.252.43
65.55.252.63
65.55.252.70
65.55.252.71
65.55.252.72
65.55.252.93
65.55.252.190
65.55.252.202

Organization: Microsoft Corporation (MSFT)
NetRange: 65.52.0.0 - 65.55.255.255
66.119.147.131

Organization: Microsoft Corporation (MSFT)
NetRange: 66.119.144.0 - 66.119.159.255
104.41.207.73
104.42.151.234

104.43.137.66
104.43.139.21
104.43.139.144
104.43.140.223
104.43.193.48
104.43.228.53
104.43.228.202
104.43.237.169
104.45.11.195
104.45.214.112
104.46.1.211
104.46.38.64
104.46.162.224
104.46.162.226

Organization: Microsoft Corporation (MSFT)
NetRange: 104.40.0.0 - 104.47.255.255
104.210.4.77
104.210.40.87
104.210.212.243
104.214.35.244
104.214.78.152

Organization: Microsoft Corporation (MSFT)
NetRange: 104.208.0.0 - 104.215.255.255
131.253.6.87
131.253.6.103

Organization: Microsoft Corp (MSFT-Z)
NetRange: 131.253.5.0 - 131.253.6.255
131.253.34.230
131.253.34.234
131.253.34.237
131.253.34.243
131.253.34.246
131.253.34.247
131.253.34.249
131.253.34.252
131.253.34.255
131.253.40.37

Organization: Microsoft Corp (MSFT-Z)
NetRange: 131.253.21.0 - 131.253.47.255

134.170.30.202
134.170.30.203
134.170.30.204
134.170.30.221
134.170.52.151
134.170.235.16

Organization: Microsoft Corp (MSFT-Z)
NetRange: 134.170.0.0 - 134.170.255.255
157.56.74.250
157.56.91.77
157.56.106.184
157.56.106.185
157.56.106.189
157.56.113.217
157.56.121.89
157.56.124.87
157.56.149.250
157.56.194.72
157.56.194.73
157.56.194.74

Organization: Microsoft Corporation (MSFT)
NetRange: 157.54.0.0 - 157.60.255.255
168.61.24.141
168.61.146.25
168.61.149.17
168.61.161.212
168.61.172.71
168.62.187.13
168.63.100.61
168.63.108.233

Organization: Microsoft Corp (MSFT-Z)
NetRange: 168.61.0.0 - 168.63.255.255
191.236.155.80
191.237.218.239
191.239.50.18
191.239.50.77
191.239.52.100
191.239.54.52
owner: Microsoft do Brasil Imp. e Com. Software e Video
G

inetnum: 191.236.0.0/14

207.68.166.254

Organization: Microsoft Corporation (MSFT)
NetRange: 207.68.128.0 - 207.68.191.255
Extra:
13.64.186.225
13.69.116.104
13.69.146.58
13.69.239.72
13.69.239.73
13.69.239.74
13.69.244.117
13.70.180.171
13.76.218.117
13.76.219.191
13.76.219.210
13.77.112.132
13.77.115.36
13.78.111.198
13.78.111.199
13.78.235.126
13.78.235.247
13.79.7.57
13.79.239.69
13.79.239.82
13.80.7.77
13.80.12.54
13.81.5.53
13.81.118.91
13.83.65.212
13.83.98.37
13.85.88.16
13.86.252.235
13.88.28.53
13.88.139.208
13.88.145.128
13.89.51.159
13.89.178.26
13.89.178.27
13.89.179.8
13.89.179.9

13.89.179.10
13.89.179.12
13.89.202.241
13.95.147.73
13.104.158.177
13.104.158.179
13.104.158.180
13.104.158.183
13.104.208.160
13.104.208.162
13.104.208.164
13.104.208.165
13.105.66.144
13.105.74.49
13.107.3.128
13.107.3.254
13.107.5.80
13.107.5.88
13.107.5.91
13.107.6.156
13.107.6.158
13.107.6.163
13.107.6.254
13.107.13.88
13.107.13.91
13.107.18.11
13.107.18.254
13.107.19.254
13.107.21.200
13.107.21.229
13.107.22.200
13.107.40.203
13.107.42.11
13.107.42.12
13.107.42.13
13.107.42.14
13.107.42.23
13.107.42.254
13.107.43.12
13.107.43.14
13.107.43.23
13.107.46.88
13.107.47.88

13.107.49.254
13.107.128.254
13.107.136.254
13.107.140.254
13.107.213.42
13.107.246.10
13.107.246.13
13.107.246.19
13.107.246.254
13.107.255.72
13.107.255.73
13.107.255.74
13.107.255.76

Organization: Microsoft Corporation (MSFT)
NetRange: 13.64.0.0 - 13.107.255.255
20.36.218.63
20.36.218.70
20.36.246.225
20.36.253.92
20.38.122.68
20.38.122.100
20.38.122.132
20.38.122.228
20.40.129.122
20.40.136.238
20.42.65.84
20.42.65.85
20.42.65.88
20.42.65.89
20.42.65.90
20.42.65.92
20.42.72.131
20.42.73.24
20.42.73.25
20.42.73.26
20.42.73.27
20.42.73.29
20.43.92.14
20.44.10.122
20.44.10.123
20.44.208.51
20.44.232.74

20.46.146.84
20.49.157.6
20.50.73.9
20.50.73.10
20.50.80.209
20.50.80.210
20.50.102.62
20.50.201.195
20.50.201.200
20.54.64.202
20.54.122.82
20.60.30.36
20.60.30.68
20.60.58.97
20.60.59.193
20.60.59.235
20.60.133.132
20.60.178.4
20.60.179.4
20.60.181.193
20.60.181.225
20.60.240.33
20.60.240.65
20.67.112.184
20.67.219.150
20.72.78.248
20.73.128.142
20.82.250.189
20.86.161.79
20.86.173.234
20.86.186.134
20.93.58.141
20.101.57.9
Organization: Microsoft Corporation (MSFT)
NetRange: 20.33.0.0 - 20.128.255.255

20.140.48.69
Organization: Microsoft Corporation (MSFT)
NetRange: 20.140.0.0 - 20.141.255.255

20.150.17.68
20.150.29.228
20.150.36.228

20.150.50.4
20.150.95.164
20.150.95.196

Organization: Microsoft Corporation (MSFT)
NetRange: 20.150.0.0 - 20.153.255.255
20.188.76.57
20.189.79.72
20.189.118.208
20.189.173.1
20.189.173.2
20.189.173.3
20.189.173.4
20.189.173.5
20.189.173.6
20.189.173.7
20.189.173.8
20.189.173.9
20.189.173.10
20.189.173.11
20.189.173.12
20.189.173.13
20.189.173.14
20.189.173.15
20.189.173.20
20.189.173.21
20.189.173.22
20.190.129.2
20.190.129.17
20.190.129.19
20.190.129.24
20.190.129.128
20.190.129.130
20.190.129.133
20.190.129.160
20.190.137.6
20.190.137.10
20.190.137.14
20.190.137.69
20.190.137.73
20.190.137.75
20.190.137.96
20.190.137.98

20.190.159.0
20.190.159.2
20.190.159.4
20.190.159.23
20.190.159.30
20.190.159.32
20.190.159.64
20.190.159.68
20.190.159.71
20.190.159.73
20.190.159.75
20.190.159.132
20.190.159.134
20.190.159.136
20.190.159.138
20.190.159.161
20.190.159.162
20.190.160.2
20.190.160.4
20.190.160.6
20.190.160.8
20.190.160.14
20.190.160.17
20.190.160.20
20.190.160.22
20.190.160.24
20.190.160.67
20.190.160.69
20.190.160.71
20.190.160.73
20.190.160.75
20.190.160.129
20.190.160.132
20.190.160.134
20.190.160.136

Organization: Microsoft Corporation (MSFT)
NetRange: 20.180.0.0 - 20.191.255.255
20.38.96.100
20.38.101.132
20.38.101.228
20.44.82.31
20.54.88.152

20.60.18.36
20.69.130.185
20.82.209.104
20.82.209.183
20.82.210.154
20.82.217.86

Organization: Microsoft Corporation (MSFT)
NetRange: 20.33.0.0 - 20.128.255.255
20.140.56.70

Organization: Microsoft Corporation (MSFT)
NetRange: 20.140.0.0 - 20.141.255.255

20.150.50.132
20.150.77.68
20.150.77.100
20.150.88.4
20.150.88.132
20.150.88.196
20.150.95.4
20.150.95.132
20.150.95.228

Organization: Microsoft Corporation (MSFT)
NetRange: 20.150.0.0 - 20.153.255.255
23.96.52.53
23.96.208.208
23.97.61.137
23.97.153.169
23.97.178.173
23.97.209.97
23.99.109.44
23.99.109.64
23.99.116.116
23.99.121.207
23.99.206.110
23.100.122.175
23.101.156.198
23.101.158.111
23.102.47.40

Organization: Microsoft Corporation (MSFT)
NetRange: 23.96.0.0 - 23.103.255.255

20.189.74.153
Organization: Microsoft Corporation (MSFT)
NetRange: 20.180.0.0 - 20.191.255.255
40.67.249.61
40.69.176.16
40.70.0.108
40.70.158.26
40.70.186.239
40.70.221.249

Organization: Microsoft Corporation (MSFT)
NetRange: 40.64.0.0 - 40.71.255.255
40.74.35.71
40.74.70.63
40.74.94.131
40.74.98.192
40.74.98.193
40.74.98.194
40.74.98.195
40.74.108.123

Organization: Microsoft Corporation (MSFT)
NetRange: 40.74.0.0 - 40.125.127.255
40.77.225.248
40.77.230.45
40.79.48.16
40.79.138.41
40.79.189.58
40.79.189.59
40.79.197.35
40.80.145.78
40.81.30.53
40.81.94.65
40.81.188.85
40.83.74.46
40.83.127.51
40.83.150.233
40.85.78.63
40.85.83.182
40.89.135.48

40.90.22.183
40.90.22.184
40.90.22.185
40.90.22.186
40.90.22.187
40.90.22.188
40.90.22.189
40.90.22.190
40.90.22.191
40.90.22.192
40.90.22.198
40.90.65.7
40.90.65.17
40.90.65.22
40.90.65.26
40.90.65.28
40.90.65.32
40.90.65.44
40.90.65.53
40.90.65.54
40.90.65.65
40.90.128.17
40.90.130.192
40.90.133.97
40.90.133.112
40.90.136.1
40.90.136.3
40.90.136.19
40.90.136.20
40.90.136.163
40.90.136.166
40.90.136.179
40.90.136.180
40.90.136.182
40.90.137.120
40.90.137.122
40.90.137.124
40.90.137.125
40.90.137.126
40.90.137.127
40.90.142.224
40.90.142.226
40.90.142.230

40.90.190.179
40.90.218.0
40.90.221.9
40.91.76.238
40.91.78.9
40.97.161.50
40.100.54.2
40.100.54.194
40.100.174.2
40.100.174.18
40.100.174.34
40.100.174.194
40.100.174.210
40.100.174.226
40.100.175.146
40.101.4.2
40.101.12.2
40.101.12.50
40.101.12.66
40.101.12.98
40.101.12.114
40.101.12.130
40.101.18.18
40.101.18.226
40.101.18.242
40.101.19.146
40.101.19.162
40.101.46.178
40.101.80.2
40.101.80.18
40.101.80.178
40.101.80.194
40.101.81.130
40.101.81.146
40.101.83.18
40.101.83.194
40.101.121.2
40.101.121.18
40.101.121.34
40.101.124.34
40.101.124.194
40.101.128.178
40.101.136.2

40.101.136.18
40.101.136.242
40.101.137.2
40.101.137.18
40.101.137.34
40.101.137.50
40.101.137.66
40.101.137.82
40.101.137.98
40.101.138.2
40.101.138.18
40.101.138.210
40.102.34.194
40.112.72.19
40.112.72.44
40.112.75.175
40.112.90.122
40.112.91.29
40.112.93.153
40.113.0.16
40.113.10.47
40.113.97.222
40.113.109.30
40.113.225.85
40.114.54.223
40.114.140.1
40.114.224.200
40.114.241.141
40.115.33.128
40.115.56.78
40.115.117.93
40.117.96.136
40.117.190.72
40.118.61.1
40.118.103.7
40.118.106.130
40.119.6.179
40.119.249.228
40.121.213.159
40.122.160.14
40.122.192.126
40.124.168.44
40.125.120.53

Organization: Microsoft Corporation (MSFT)
NetRange: 40.74.0.0 - 40.125.127.255
40.126.1.128
40.126.1.130
40.126.1.142
40.126.1.145
40.126.1.166
40.126.9.5
40.126.9.6
40.126.9.8
40.126.9.66
40.126.9.73
40.126.9.77
40.126.31.1
40.126.31.4
40.126.31.6
40.126.31.8
40.126.31.67
40.126.31.69
40.126.31.71
40.126.31.73
40.126.31.135
40.126.31.137
40.126.31.139
40.126.31.141
40.126.31.143
40.126.31.163
40.126.31.164
40.126.32.68
40.126.32.72
40.126.32.74
40.126.32.76
40.126.32.133
40.126.32.134
40.126.32.136
40.126.32.138
40.126.32.140

Organization: Microsoft Corporation (MSFT)
NetRange: 40.126.0.0 - 40.126.63.255
40.127.128.174
40.127.142.76
40.127.195.156

40.127.240.158
40.127.243.65

Organization: Microsoft Corporation (MSFT)
NetRange: 40.126.128.0 - 40.127.255.255
51.11.168.160
51.11.168.232

Microsoft Limited UK
inetnum: 51.10.0.0 - 51.13.255.255
51.104.15.252
51.104.15.253
51.104.139.180
51.104.144.132
51.104.146.109
51.105.71.136
51.105.71.137
51.105.208.173
51.105.236.244

descr: Microsoft Limited UK
inetnum: 51.103.0.0 - 51.105.255.255

51.116.232.21
descr: Microsoft Limited UK
inetnum: 51.116.0.0 - 51.116.255.255

51.124.78.146
descr: Microsoft Limited UK
51.124.0.0 - 51.124.255.255

51.132.193.104
51.132.193.105
51.132.208.181

descr: Microsoft Limited UK
inetnum: 51.132.0.0 - 51.132.255.255
51.136.15.177
51.136.37.147
51.137.137.111
51.138.106.75

descr: Microsoft Limited UK

inetnum: 51.136.0.0 - 51.138.255.255
51.140.65.84
51.140.98.69
51.140.127.197
51.141.26.229
51.141.32.51
51.141.118.220
51.141.166.104
51.143.49.132
51.144.108.120
51.144.113.175
51.145.123.29

Microsoft Limited UK
inetnum: 51.140.0.0 - 51.145.255.255
52.97.129.66
52.97.129.226
52.97.129.242
52.97.133.146
52.97.133.162
52.97.133.178
52.97.133.194
52.97.133.210
52.97.133.226
52.97.133.242
52.97.135.114
52.97.144.2
52.97.146.34
52.97.146.130
52.97.146.162
52.97.146.194
52.97.146.210
52.97.150.2
52.97.151.50
52.97.151.82
52.97.152.114
52.97.155.114
52.97.158.162
52.97.163.2
52.97.170.34
52.97.171.194
52.97.179.194
52.97.179.226

52.97.179.242
52.97.186.114
52.97.188.66
52.97.189.98
52.97.200.130
52.97.200.146
52.97.200.178
52.97.201.2
52.97.201.18
52.97.201.34
52.97.201.50
52.97.201.66
52.97.201.98
52.97.208.18
52.97.208.50
52.97.211.66
52.97.211.82
52.97.211.98
52.97.211.114
52.97.211.130
52.97.211.146
52.97.211.162
52.97.211.178
52.97.211.194
52.97.211.210
52.97.211.226
52.97.211.242
52.97.212.82
52.97.212.98
52.97.212.114
52.97.215.98
52.97.219.194
52.97.219.210
52.97.219.226
52.97.219.242
52.97.232.194
52.97.233.2
52.97.233.18
52.97.233.34
52.97.233.50
52.97.233.66
52.97.233.82
52.97.233.98

52.97.233.114
52.97.241.162
52.97.241.178
52.97.250.194
52.97.250.226
52.98.5.194
52.98.42.194
52.98.66.98
52.98.145.66
52.98.145.82
52.98.145.98
52.98.145.114
52.98.151.226
52.98.151.242
52.98.207.130
52.98.207.146
52.98.207.162
52.109.8.19
52.109.8.20
52.109.8.21
52.109.12.18
52.109.12.19
52.109.12.20
52.109.12.21
52.109.12.22
52.109.12.23
52.109.12.24
52.109.28.63
52.109.28.107
52.109.32.23
52.109.32.63
52.109.68.14
52.109.68.21
52.109.76.8
52.109.76.30
52.109.76.31
52.109.76.32
52.109.76.33
52.109.76.34
52.109.76.35
52.109.76.36
52.109.76.40
52.109.76.68

52.109.76.124
52.109.88.6
52.109.88.10
52.109.88.34
52.109.88.35
52.109.88.36
52.109.88.37
52.109.88.38
52.109.88.39
52.109.88.40
52.109.88.44
52.109.88.174
52.109.120.17
52.109.120.18
52.109.120.19
52.109.120.20
52.109.120.21
52.109.120.22
52.109.120.23
52.109.124.18
52.109.124.19
52.109.124.20
52.109.124.21
52.109.124.22
52.109.124.23
52.109.124.24

Organization: Microsoft Corporation (MSFT)
52.96.0.0/12, 52.112.0.0/14
52.113.194.131
52.113.194.132
52.113.195.132
52.113.196.254
52.114.6.46
52.114.6.47
52.114.7.36
52.114.7.37
52.114.7.38
52.114.7.39
52.114.20.14
52.114.20.18
52.114.32.5
52.114.32.6

52.114.32.7
52.114.32.8
52.114.32.24
52.114.32.25
52.114.36.1
52.114.36.2
52.114.36.3
52.114.36.4
52.114.74.43
52.114.74.44
52.114.74.45
52.114.75.78
52.114.75.79
52.114.75.149
52.114.75.150
52.114.76.34
52.114.76.35
52.114.76.37
52.114.77.33
52.114.77.34
52.114.77.137
52.114.77.164
52.114.88.19
52.114.88.20
52.114.88.21
52.114.88.22
52.114.88.28
52.114.88.29
52.114.128.7
52.114.128.8
52.114.128.9
52.114.128.10
52.114.128.43
52.114.128.44
52.114.128.58
52.114.128.69
52.114.128.70
52.114.128.71
52.114.128.72
52.114.128.73
52.114.128.74
52.114.128.75
52.114.132.11

52.114.132.12
52.114.132.14
52.114.132.20
52.114.132.21
52.114.132.22
52.114.132.23
52.114.132.34
52.114.132.47
52.114.132.73
52.114.132.74
52.114.132.91
52.114.133.60
52.114.133.61
52.114.158.50
52.114.158.51
52.114.158.52
52.114.158.53
52.114.158.91
52.114.158.92
52.114.158.102
52.114.159.22
52.114.159.23
52.114.159.32
52.114.159.33
52.114.159.34
52.114.159.35
52.114.159.112

Organization: Microsoft Corporation (MSFT)
NetRange: 52.96.0.0 - 52.115.255.255
52.136.230.174
52.138.148.87
52.138.148.89
52.138.148.159
52.138.216.83
52.142.80.173
52.142.84.61
52.142.114.2
52.142.114.176
52.142.119.134

Organization: Microsoft Corporation (MSFT)
NetRange: 52.132.0.0 - 52.143.255.255

52.154.66.52
52.154.67.2
52.154.67.56
52.155.172.105
52.156.41.171
52.156.48.67
52.156.146.245
52.156.196.151
52.156.204.185
52.158.24.209
52.158.24.229
52.158.25.39
52.158.238.42
52.159.49.192
52.163.118.68
52.164.191.55
52.164.227.208
52.164.251.44
52.166.110.64
52.166.110.215
52.166.120.77
52.165.136.32
52.167.18.95
52.167.88.112
52.167.249.196
52.168.24.174
52.168.112.66
52.168.112.67
52.168.117.169
52.168.117.170
52.168.117.173
52.169.71.150
52.170.57.27
52.170.194.77
52.171.136.200
52.173.152.64
52.175.30.196
52.176.224.96
52.178.17.2
52.178.17.3
52.178.161.41
52.178.163.85
52.178.178.16

52.178.182.73
52.178.193.116
52.179.13.204
52.182.143.208
52.182.143.210
52.182.143.211
52.182.143.212
52.183.24.194
52.183.104.36
52.184.81.210
52.184.82.129
52.184.92.48
52.184.168.116
52.184.220.11
52.186.25.68
52.188.77.27

Organization: Microsoft Corporation (MSFT)
52.154.66.52
52.224.75.92
52.225.136.36
52.225.255.33
52.230.10.183
52.230.240.94
52.231.32.10
52.232.16.77
52.232.19.76
52.232.69.150
52.233.164.195
52.233.199.249
52.239.137.4
52.239.156.2
52.239.156.74
52.239.156.138
52.239.172.132
52.239.172.164
52.239.175.68
52.239.177.36
52.239.177.100
52.239.177.228
52.239.150.170
52.239.151.138
52.239.151.170

52.239.156.2
52.239.157.138
52.239.157.202
52.239.174.4
52.239.174.132
52.239.174.196
52.239.174.228
52.239.175.4
52.239.177.68
52.239.184.10
52.239.184.42
52.239.198.228
52.239.207.100
52.239.222.100
52.239.223.19
52.239.223.132
52.239.234.100
52.239.234.228
52.239.235.100
52.247.37.26
52.255.148.73

Organization: Microsoft Corporation (MSFT)
NetRange: 52.224.0.0 - 52.255.255.255
64.4.16.212
64.4.16.214
64.4.16.216
64.4.16.218
64.4.54.18
64.4.54.22
64.4.54.253
64.4.54.254

Organization: Microsoft Corporation (MSFT)
NetRange: 64.4.0.0 - 64.4.63.255
65.52.98.231
65.52.226.14
65.54.187.128
65.54.187.130
65.54.187.131
65.54.187.132
65.54.187.134
65.54.198.196

65.55.44.51
65.55.44.54
65.55.44.108
65.55.44.109
65.55.108.23
65.55.130.50

Organization: Microsoft Corporation (MSFT)
NetRange: 65.52.0.0 - 65.55.255.255
104.40.144.210
104.40.159.215
104.40.210.32
104.40.211.35
104.41.219.140
104.42.41.237
104.42.191.226
104.43.203.255
104.44.80.172
104.44.88.24
104.44.88.28
104.44.88.103
104.45.18.177
104.46.91.34

Organization: Microsoft Corporation (MSFT)
NetRange: 104.40.0.0 - 104.47.255.255
104.208.16.88
104.208.16.89
104.208.16.90
104.208.16.94
104.208.248.16
104.209.172.133
104.210.62.125
104.211.73.16
104.211.91.221
104.211.93.71
104.211.96.15
104.212.67.88
104.212.67.92
104.212.67.142
104.212.67.154
104.212.67.162
104.212.67.168

104.212.67.187
104.212.67.188
104.212.67.223
104.212.67.234
104.212.67.245
104.214.77.221
104.214.150.122
104.214.220.181
104.215.146.200

Organization: Microsoft Corporation (MSFT)
NetRange: 104.208.0.0 - 104.215.255.255
131.253.14.227
131.253.14.229
131.253.14.230
131.253.14.231
131.253.33.200
131.253.33.203
131.253.33.219
131.253.33.254

Organization: Microsoft Corp (MSFT-Z)
NetRange: 131.253.12.0 - 131.253.18.255
134.170.178.97
134.170.185.70
134.170.188.248

Organization: Microsoft Corp (MSFT-Z)
NetRange: 134.170.0.0 - 134.170.255.255
137.116.44.10
137.116.234.82

Organization: Microsoft Corp (MSFT-Z)
NetRange: 137.116.0.0 - 137.116.255.255
137.117.142.136
137.117.144.39
137.117.228.253
137.117.235.16
137.117.243.30

Organization: Microsoft Corp (MSFT-Z)
NetRange: 137.117.0.0 - 137.117.255.255
137.135.251.63

OrgName: Microsoft Corp
NetRange: 137.135.0.0 - 137.135.255.255
138.91.136.108
138.91.122.49
138.91.140.216
138.91.141.104

Organization: Microsoft Corp (MSFT-Z)
NetRange: 138.91.0.0 - 138.91.255.255
157.55.109.7
157.55.109.224
157.55.109.226
157.55.109.228
157.55.109.230
157.55.109.232
157.55.129.21
157.55.134.136
157.55.134.138
157.55.134.140
157.55.134.142
157.55.135.128
157.55.135.130
157.55.135.132
157.55.135.134
157.56.57.5

Organization: Microsoft Corporation (MSFT)
NetRange: 157.54.0.0 - 157.60.255.255
168.62.57.154
168.62.58.130
168.62.200.169
168.63.18.79
168.63.67.155
168.63.102.42

Organization: Microsoft Corp (MSFT-Z)
NetRange: 168.61.0.0 - 168.63.255.255
191.237.208.126
191.239.213.197

owner: Microsoft do Brasil Imp. e Com. Software e Video
G
inetnum: 191.236.0.0/14

204.152.141.244

Organization: Microsoft Corp (MSFT-Z)
NetRange: 204.152.140.0 - 204.152.141.255

207.46.7.252
207.46.26.12
207.46.26.14
207.46.26.16
207.46.26.18
207.46.101.29
207.46.153.155
207.46.194.14
207.46.194.25
207.46.194.33
207.46.194.40
207.46.223.94

Organization: Microsoft Corporation (MSFT)
NetRange: 207.46.0.0 - 207.46.255.255
Update:
13.68.87.47
13.68.87.175
13.68.88.129
13.68.93.109
13.74.179.117
13.78.168.230
13.78.177.144
13.78.179.199
13.78.180.50
13.78.180.90
13.78.184.44
13.78.184.186
13.78.186.254
13.78.187.58
13.78.230.134
13.83.148.218
13.83.148.235
13.83.149.5
13.83.149.67
13.83.151.160
13.86.124.174
13.86.124.184

13.86.124.191
13.91.16.64
13.91.16.65
13.91.16.66
13.91.16.67
13.91.16.68
13.91.16.69
13.91.16.70
13.91.16.71
13.92.211.120
13.107.4.50
13.107.4.52
13.107.4.254

Organization: Microsoft Corporation (MSFT)
NetRange: 13.64.0.0 - 13.107.255.255
20.36.222.39
20.36.252.130
20.41.41.23
20.42.24.29
20.42.24.50
20.44.77.24
20.44.77.45
20.44.77.49
20.44.77.219
20.45.4.77
20.45.4.178
20.54.24.69
20.54.24.79
20.54.24.148
20.54.24.169
20.54.24.231
20.54.24.246
20.54.25.4
20.54.25.16
20.54.89.15
20.54.89.106
20.54.110.119
20.54.110.249
20.62.190.184
20.62.190.185
20.62.190.186
20.62.190.187

20.62.190.188
20.62.190.189
20.62.190.190
20.62.190.191
20.83.81.160
20.83.81.161
20.83.81.162
20.83.81.163
20.83.81.164
20.83.81.165
20.185.109.208
20.186.48.46
20.188.74.161
20.188.78.184
20.188.78.185
20.188.78.187
20.188.78.188
20.188.78.189
20.190.3.175
20.190.9.86
20.191.46.109
20.191.46.211
20.199.120.85
20.199.120.151
20.199.120.182

Organization: Microsoft Corporation (MSFT)
NetRange: 20.33.0.0 - 20.128.255.255
23.103.189.125
23.103.189.126
23.103.189.157
23.103.189.158

Organization: Microsoft Corporation (MSFT)
NetRange: 23.96.0.0 - 23.103.255.255
40.67.248.104
40.67.251.132
40.67.251.134
40.67.252.175
40.67.252.206
40.67.253.249
40.67.254.36
40.67.254.97

40.67.255.199
40.69.216.73
40.69.216.129
40.69.216.251
40.69.218.62
40.69.219.197
40.69.220.46
40.69.221.239
40.69.222.109
40.69.223.39
40.69.223.198
40.70.224.144
40.70.224.145
40.70.224.147
40.70.224.148
40.70.224.149
40.70.229.150

Organization: Microsoft Corporation (MSFT)
NetRange: 40.64.0.0 - 40.71.255.255
40.77.18.167
40.77.224.8
40.77.224.11
40.77.224.145
40.77.224.254
40.77.226.13
40.77.226.181
40.77.226.246
40.77.226.247
40.77.226.248
40.77.226.249
40.77.226.250
40.77.229.8
40.77.229.9
40.77.229.12
40.77.229.13
40.77.229.16
40.77.229.21
40.77.229.22
40.77.229.24
40.77.229.26
40.77.229.27
40.77.229.29

40.77.229.30
40.77.229.32
40.77.229.35
40.77.229.38
40.77.229.44
40.77.229.45
40.77.229.50
40.77.229.53
40.77.229.62
40.77.229.65
40.77.229.67
40.77.229.69
40.77.229.70
40.77.229.71
40.77.229.74
40.77.229.76
40.77.229.80
40.77.229.81
40.77.229.82
40.77.229.88
40.77.229.118
40.77.229.123
40.77.229.128
40.77.229.133
40.77.229.141
40.77.229.199
40.79.65.78
40.79.65.123
40.79.65.235
40.79.65.237
40.79.66.194
40.79.66.209
40.79.67.176
40.79.70.158
40.91.73.169
40.91.73.219
40.91.75.5
40.91.80.89
40.91.91.94
40.91.120.196
40.91.122.44
40.125.122.151
40.125.122.176

Organization: Microsoft Corporation (MSFT)
NetRange: 40.74.0.0 - 40.125.127.255
51.103.5.159
51.103.5.186
51.104.162.50
51.104.162.168
51.104.164.114
51.104.167.48
51.104.167.186
51.104.167.245
51.104.167.255
51.105.249.223
51.105.249.228
51.105.249.239

descr: Microsoft Limited UK
inetnum: 51.103.0.0 - 51.105.255.255
52.142.21.136
52.137.102.105
52.137.103.96
52.137.103.130
52.137.110.235
52.142.21.137
52.142.21.139
52.142.21.140
52.142.21.141
52.143.80.209
52.143.81.222
52.143.84.45
52.143.86.214
52.143.87.28

Organization: Microsoft Corporation (MSFT)
NetRange: 52.132.0.0 - 52.143.255.255
52.147.176.8
52.148.148.114
52.152.108.96
52.152.110.14
52.155.95.90
52.155.115.56
52.155.169.137
52.155.183.99
52.155.217.156

52.155.223.194
52.156.144.83
52.158.114.119
52.158.122.14
52.161.15.246
52.164.221.179
52.164.226.245
52.167.222.82
52.167.222.147
52.167.223.135
52.169.82.131
52.169.83.3
52.169.87.42
52.169.123.48
52.175.23.79
52.177.164.251
52.177.247.15
52.178.192.146
52.179.216.235
52.179.219.14
52.183.47.176
52.183.118.171
52.184.152.136
52.184.155.206
52.184.212.181
52.184.213.21
52.184.213.187
52.184.214.53
52.184.214.123
52.184.214.139
52.184.216.174
52.184.216.226
52.184.216.246
52.184.217.20
52.184.217.37
52.184.217.56
52.187.60.107
52.188.72.233

Organization: Microsoft Corporation (MSFT)
NetRange: 52.145.0.0 - 52.191.255.255
52.226.130.114
52.229.170.171

52.229.170.224
52.229.171.86
52.229.171.202
52.229.172.155
52.229.174.29
52.229.174.172
52.229.174.233
52.229.175.79
52.230.216.17
52.230.216.157
52.230.220.159
52.230.223.92
52.230.223.167
52.232.225.93
52.238.248.1
52.238.248.2
52.238.248.3
52.238.248.4
52.238.248.5
52.238.248.6
52.238.248.7
52.242.97.97
52.242.101.226
52.242.231.32
52.242.231.33
52.242.231.35
52.242.231.36
52.242.231.37
52.243.153.146
52.248.96.36
52.249.24.101
52.249.36.200
52.249.36.205
52.249.36.206
52.249.36.207
52.249.58.51
52.250.46.232
52.250.46.237
52.250.46.238
52.250.195.200
52.250.195.204
52.250.195.206
52.250.195.207

52.251.79.25
52.253.130.84
52.254.106.61
52.254.114.64
52.254.114.65
52.254.114.67
52.254.114.68
52.254.114.69
52.254.114.70
52.254.114.71

Organization: Microsoft Corporation (MSFT)
NetRange: 52.224.0.0 - 52.255.255.255
64.4.27.50

Organization: Microsoft Corporation (MSFT)
NetRange: 64.4.0.0 - 64.4.63.255
65.52.108.29
65.52.108.33
65.52.108.59
65.52.108.90
65.52.108.92
65.52.108.153
65.52.108.154
65.52.108.185
65.55.242.254

Organization: Microsoft Corporation (MSFT)
NetRange: 65.52.0.0 - 65.55.255.255
66.119.144.157
66.119.144.158
66.119.144.189
66.119.144.190

Organization: Microsoft Corporation (MSFT)
NetRange: 66.119.144.0 - 66.119.159.255
67.26.27.254

Organization: Level 3 Parent, LLC (LPL-141)
NetRange: 67.24.0.0 - 67.31.255.255
104.45.177.233

Organization: Microsoft Corporation (MSFT)

NetRange: 104.40.0.0 - 104.47.255.255
111.221.29.40

descr: Microsoft Corp, Singapore
inetnum: 111.221.29.0 - 111.221.29.255
134.170.51.187
134.170.51.188
134.170.51.190
134.170.51.246
134.170.51.247
134.170.51.248
134.170.53.29
134.170.53.30
134.170.115.55
134.170.115.56
134.170.115.60
134.170.115.62
134.170.165.248
134.170.165.249
134.170.165.251
134.170.165.253

Organization: Microsoft Corp (MSFT-Z)
NetRange: 134.170.0.0 - 134.170.255.255
137.135.62.92\

Organization: Microsoft Corp (MSFT-Z)
NetRange: 137.135.0.0 - 137.135.255.255
157.55.133.204
157.55.240.89
157.55.240.126
157.55.240.220
157.56.77.138
157.56.77.139
157.56.77.140
157.56.77.141
157.56.77.148
157.56.77.149
157.56.96.54
157.56.96.58
157.56.96.123
157.56.96.157

Organization: Microsoft Corporation (MSFT)
NetRange: 157.54.0.0 - 157.60.255.255
191.232.80.53
191.232.80.58
191.232.80.60
191.232.80.62
191.232.139.2
191.232.139.182
191.232.139.253
191.232.139.254
191.234.72.183
191.234.72.186
191.234.72.188
191.234.72.190

owner: Microsoft do Brasil Imp. e Com. Software e Video
G
inetnum: 191.232.0.0/14
207.46.114.58
207.46.114.61

Organization: Microsoft Corporation (MSFT)
NetRange: 207.46.0.0 - 207.46.255.255

Netstat

Use the Netstat command to display stack settings, and information about open ports and established connections.

Opened port and services using Netstat -

Netstat also returns network service statistics.

I would like to suggest you investigate the IP address from destination in the "Netstat -a" result is used for which service or this IP address belongs to which device.

Ping

Ping (IP or domain name) with -t provides continuous pings.

References:

https://security.stackexchange.com/questions/119469/does-windows-10-leak-information-about-your-ip-address

https://www.comparitech.com/blog/vpn-privacy/prevent-ip-leaks/

https://sectigostore.com/blog/ip-leak-test-quick-tips-to-check-whether-your-ip-is-leaking/

Wireshark

What is Wireshark?

Wireshark is Open Source Software released under the GNU General Public License.

Install Wireshark and set it to capture from your Ethernet or Wi-Fi network interface. (also can work with USB wireless adaptors)

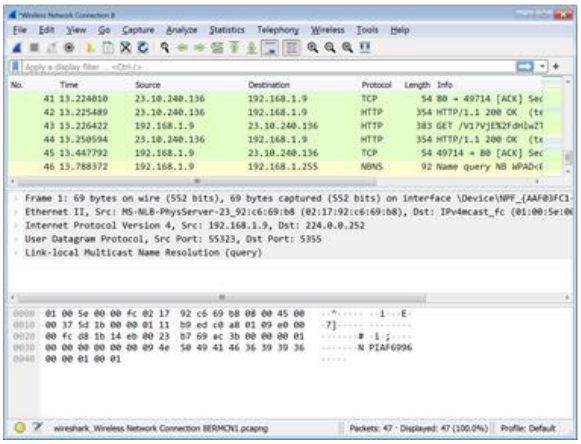
Wireshark is the world's most popular network protocol analyzer. It is used for troubleshooting, analysis, development and education.

Note: It is an essential tool for those who work in cybersecurity.

Check the main page at:

https://www.wireshark.org

For more information on its use check out YouTube videos.



Wireshark will show only unencrypted packets.

Note: Microsoft's Windows 10/11 telemetry is encrypted using TLS v1.2, and so there's no way of actually seeing the content of a telemetry packet.

Windows 10's telemetry is not sending vast amounts of your personal data - it's sending small snippets of information and that to a set of servers with names and IP addresses that can easily be blacklisted at a router if you really want to keep your network traffic private. Remember that not all packets contain data.

https://www.zdnet.com/article/windows-10-and-telemetry-time-for-a-simple-network-analysis/

From the screen shot above:

224.0.0.252 MCAST-NET

239.255.255.250 MCAST-NET

224.0.0.252 MCAST-NET

mcast.net is a second level domain reserved by the Internet Assigned Numbers Authority (IANA) and maintained by Verisign used to bind DNS records unique to multicast addressing. The domain and its subdomains are not associated with any web site.

142.250.190.131 GOOGLE

Search the world's information, including webpage's, images, videos and more.

23.76.205.27 AKAMAI

23.10.240.136 AKAMAI

Akamai Technologies, Inc. is an American content delivery network (CDN), a Cybersecurity, and cloud service company, providing web and Internet security services.

Think your Data is Safe in the Cloud?

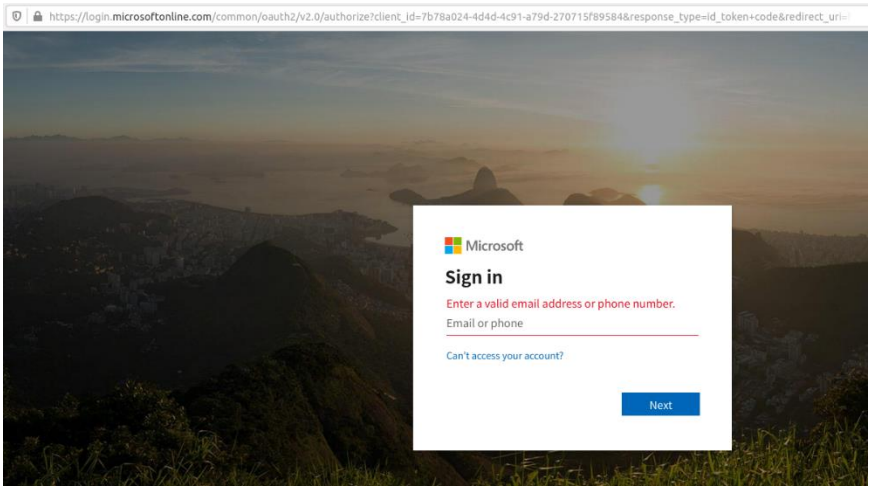
You are not Safe in the Cloud! How can Microsoft Azure, MS OneDrive, and Google AWS protect your systems and data, if they cannot protect their own? What follows is a summary and de-geekification of the information in the enclosed hyperlinks in an attempt to make it more understandable for the non-geek readers.

Cloud Identity is promoted as a great thing these days. You can sign up to lots of services using your social identity from Facebook, Google, or from Microsoft. You do not have to invent new passwords (or reuse passwords used elsewhere), and you get easy Single Sign On. This is sold as having more advantages than drawbacks for users, with little awareness of some of the dangers.

Think two factor authentication will protect you in the cloud. Think again. Even if an organization requires multi-factor authentication at sign-in, recall that a malware login process can take place on Microsoft's own Web site. In fact, many of these malicious actors host their evil doing directly on Microsoft Azure sites. That means having two-factor enabled for an account would do nothing to prevent a malicious app that has already been approved by the user from accessing their emails or files. They use malicious a Microsoft Office 365 App to gain access to a victim's account without requiring them to give up their credentials to the attackers.

This is a long and fairly complex technical read, but if you are a business using cloud services, you better have your tech guys read this.

Late last year saw the re-emergence of a nasty phishing tactic that allows the attacker to gain full access to a user's data stored in the cloud without actually stealing the account password. The phishing lure starts with a link that leads to the real login page for a cloud email and/or file storage service. Anyone who takes the bait will inadvertently forward a digital token to the attackers that gives them indefinite access to the victim's email, files, and contacts — even after the victim has changed their password.



Let us define what phishing is.

Phishing is using social engineering techniques to deceive computer and Internet users. These users are often lured into this by communications or prompts purporting to be from trusted parties.

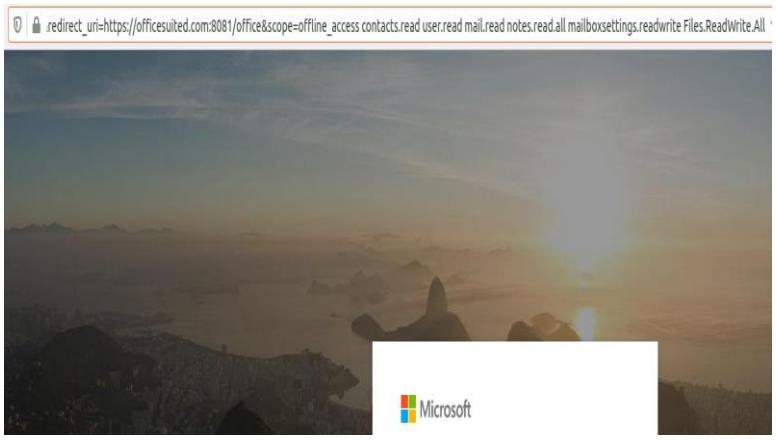
While the most recent phishing attacks target corporate users of Microsoft's Office 365 service, the same approach can be leveraged to attack users of many other cloud providers. In 2017, a similar technique was used to plunder accounts at Google's Gmail service.

Security experts have identified a malicious link which took people who clicked to an official Office 365 login page—**login.microsoftonline.com** someplace else. Anyone suspicious about the link would have seen nothing immediately amiss in their browser's address bar, and could easily verify that the link indeed took them to Microsoft's real login page. See browser address bar below.

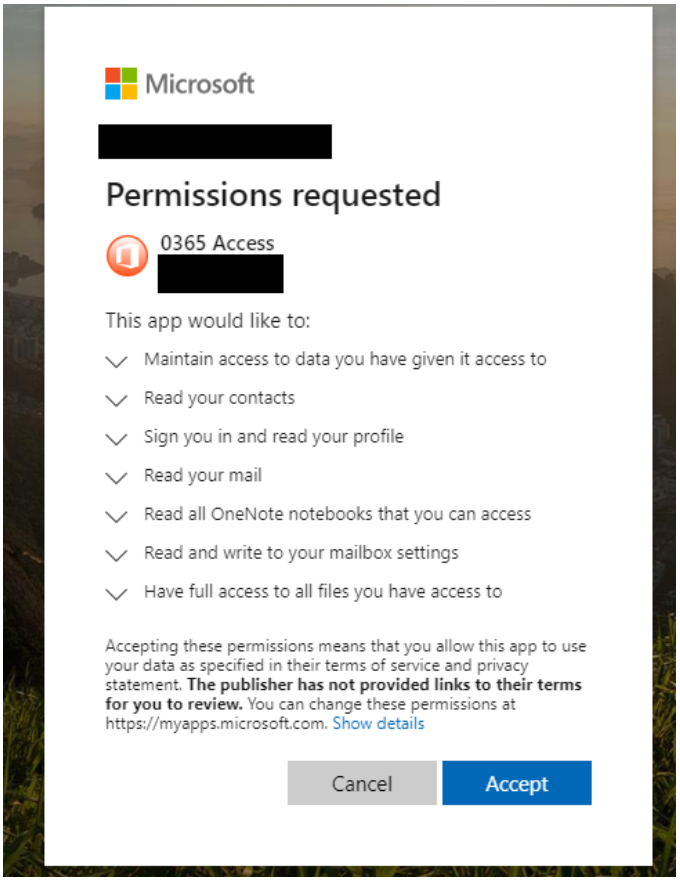
This phishing link asks users to log in at Microsoft's real Office 365 portal (login.microsoftonline.com).

Only by copying and pasting the link or by scrolling far to the right in the URL bar could you detect that something isn't quite right:

Notice this section of the URL (obscured off-page and visible only by scrolling to the right quite a bit) attempts to grant a malicious app hosted at officesuited.com full access to read the victim's email and files stored at Microsoft's Office 365 service.


:redirect_uri=https://officesuited.com:8081/office&scope=offline_access contacts.read user.read mail.read notes.read.all mailboxsettings.readwrite Files.ReadWrite.All
Microsoft

As we can see from the URL in the image directly above, the link tells Microsoft to forward the authorization token produced by a successful login to the domain ***officesuited[.]com****. From there, the user will be presented with a prompt that says an app is requesting permissions to read your email, contacts, OneNote notebooks, access your files, read/write to your mailbox settings, sign you in, read your profile, and maintain access to that data.*


Microsoft
[redacted]
Permissions requested
0365 Access
[redacted]
This app would like to:
Maintain access to data you have given it access to
Read your contacts
Sign you in and read your profile
Read your mail
Read all OneNote notebooks that you can access
Read and write to your mailbox settings
Have full access to all files you have access to
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. The publisher has not provided links to their terms for you to review. You can change these permissions at https://myapps.microsoft.com. Show details
Cancel
Accept

The app that generated this request was created using information stolen from a legitimate organization. The domain hosting the malicious app pictured above — **officemtr[.]com** — is hosted at the same Internet address as officesuited[.]com and likely signed using the same legitimate company's credentials.

These attackers are exploiting a feature of Outlook known as "add-ins," which are applications built by third-party developers that can be installed either from a file or URL from the Office store. By default, any user can apply add-ins to their outlook application as Microsoft allows Office 365 add-ins and apps to be installed via side loading without going through the Office Store, and thereby avoiding any review process.

This attack method is more like malware than traditional phishing, which tries to trick someone into giving their password to the scammers. Instead of handing off credentials to someone, they are allowing an outside application to start interacting with their Office 365 environment directly. How could the user somehow understand that there is a malicious third party involved in this transaction, when the site *is* legitimate, and at that point, their guard is down?

The scary part about this attack is that once a user grants the malicious app permissions to read their files and emails, the attackers can maintain access to the account after the user changes his password. Only system administrators responsible can see that the app had been approved.

Once given permission to access the user's email and files, the app will retain that access until one of two things happen: Microsoft discovers and disables the malicious app, or an administrator on the victim user's domain removes the program from the user's account.

Expecting swift action from Microsoft might not be ideal: From my testing, Microsoft appears to have disabled the malicious app being served from officesuited[.]com sometime around Dec. 19 — roughly one week after it went live.

In a statement provided to KrebsOnSecurity, Microsoft Senior Director Jeff Jones said the company continues to monitor for potential new variations of this malicious activity and will take action to disable applications as they are identified.

"The technique described relies on a sophisticated phishing campaign that invites users to permit a malicious Azure Active Directory Application," Jones said. "We've notified impacted customers and worked with them to help remediate their environments."

Microsoft's instructions for detecting and removing illicit consent grants in Office 365 are here. Microsoft says administrators can enable a setting that blocks users from installing third-party apps into Office 365, but calls this a "drastic step" that "isn't recommended as it severely impairs users' ability to be productive with third-party applications."

PhishLabs' Tyler said he disagrees with Microsoft here, and encourages Office 365 administrators to block users from installing apps altogether — or at the very least restrict them to apps from the official Microsoft store.

Apart from that, he said, it is important for Office 365 administrators to periodically look for suspicious apps installed on their Office 365 environment.

"If an organization were to fall prey to this, your traditional methods of eradicating things involve activating two-factor authentication, clearing the user's sessions, and so on, but that won't do anything here," he said. "It's important that response teams know about this tactic so they can look for problems. If you can't or don't want to do that, at least make sure you have security logging turned on so it's generating an alert when people are introducing new software into your infrastructure."

Do not take my word for any of this; here are some comments from the web:

"I personally have seen Microsoft account phishing sites hosted on Azure."

"App permissions page? The unfortunate thing is that people do not read those and just blindly hit "Accept."

"Over 90% of security incidents are caused by either people doing something they shouldn't do, or someone not doing something they should do. Humans are not perfect, shocking, I know, but it is true. The brightest people in the world, yes even "security experts" can fall for a scam if you catch them at the right time."

"The root cause is the many years that Microsoft has taught users to click by rote": Next > Next > Next ….", "OK > OK > OK….", "I Agree > I Agree > I Agree…", "Accept > Accept > Accept…"

"The "Cloud" is getting darker by the day. I wonder if this is huge rigged three card Monty scam or a well-choreographed multinational confidence game. I am dubious MS is actually putting their customer's security over their corporate profits. Data harvesting seems to be a big winner for certain big players these days."

"First, while the most recent versions of this stealthy phish targeted corporate users of Microsoft's Office 365 service, the same approach could be leveraged to ensnare users of many other cloud providers. Second, this attack is not exactly new: In 2017, for instance, phishers used a similar technique to plunder accounts at Google's Gmail service."

"The link contains standard OAuth functionality: – it directs Microsoft to give access to the users' resources to a consumer (in this case, the attacker)– Microsoft correctly asks the users if they're ok with this– The users reply "yes", granting the attacker access"

"Really the only cleverness here is getting the user in a context where such a prompt is not unexpected, therefore multiplying the chances that the users will click "yes".

"Seems like bullet hole in Microsoft's cloud."

We should all be concerned about this.

Sources:

https://krebsonsecurity.com/2020/01/tricky-phish-angles-for-persistence-not-passwords/ - more-50056

https://securityintheenterprise.blogspot.com/2019/11/microsoft-azuread-and-office365-not.html

https://info.phishlabs.com/blog/office-365-phishing-uses-malicious-app-persist-password-reset

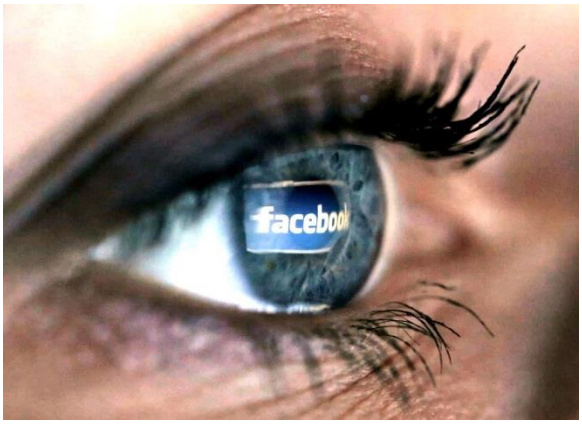
https://duo.com/blog/gmail-oauth-phishing-goes-viral

https://krebsonsecurity.com/2020/01/phishing-for-apples-bobbing-for-links/

NSA NETWORK INFRASTRUCTURE SECURITY GUIDANCE

Download the PDF

https://www.cisa.gov/uscert/ncas/current-activity/2022/03/03/nsa-releases-network-infrastructure-security-guidance



What data Facebook (Meta) collects

For those who have the naïve view that they have nothing to hide, below is a sample of what just Facebook alone collects:

Targeting options for Facebook advertisers

1. Location, via GPS or if turned off, via local cell towers
2. Age
3. Generation
4. Gender
5. Language
6. Education level
7. Field of study
8. School
9. Ethnic affinity
10. Income and net worth
11. Home ownership and type
12. Home value
13. Property size
14. Square footage of home
15. Year home was built
16. Household composition
17. Users who have an anniversary within 30 days
18. Users who are away from family or hometown
19. Users who are friends with someone who has an anniversary, is newly married, or engaged, recently moved, or has an upcoming birthday
20. Users in long-distance relationships
21. Users in new relationships
22. Users who have new jobs
23. Users who are newly engaged

24. Users who are newly married
25. Users who have recently moved
26. Users who have birthdays soon
27. Parents
28. Expectant parents
29. Mothers divided by "type" (soccer, trendy, etc.)
30. Users who are likely to engage in politics
31. Conservatives and liberals
32. Relationship status
33. Employer
34. Industry
35. Job title
36. Office type
37. Interests
38. Users who own motorcycles
39. Users who plan to buy a car (and what kind/brand of car, and how soon)
40. Users who bought auto parts or accessories recently
41. Users who are likely to need auto parts or services
42. Style and brand of car you drive
43. Year car was bought
44. Age of car
45. How much money user is likely to spend on next car?
46. Where user is likely to buy next car
47. How many employees your company has
48. Users who own small businesses
49. Users who work in management or are executives
50. Users who have donated to charity (divided by type)
51. Operating system on your computer
52. Users who play canvas games
53. Users who own a gaming console
54. Users who have created a Facebook event
55. Users who have used Facebook Payments
56. Users who have spent more than average on Facebook Payments
57. Users who administer a Facebook page
58. Users who have recently uploaded photos to Facebook
59. Internet browser
60. Email service
61. Early/late adopters of technology
62. Expats (divided by country they are from originally)
63. Users who belong to a credit union, national bank, or regional bank

64. Users who investor (divided by investment type)
65. Number of credit lines
66. Users who are active credit card users
67. Credit card type
68. Users who have a debit card
69. Users who carry a balance on their credit card
70. Users who listen to the radio
71. Preference in TV shows
72. Users who use a mobile device (divided by brand)
73. Internet connection type
74. Users who recently acquired a smartphone or tablet
75. Users who access the Internet via a smartphone or tablet
76. Users who use coupons
77. Types of clothing user's household buys
78. Time of year user's household shops most
79. Users who are "heavy" buyers of beer, wine, or spirits
80. Users who buy groceries (and what kinds)
81. Users who buy beauty products
82. Users who buy allergy medications, cough/cold medications, pain relief products, and over-the-counter meds
83. Users who spend money on household products
84. Users who spend money on products for kids or pets, and what kinds of pets
85. Users whose household makes more purchases than is average
86. Users who tend to shop online (or off)
87. Types of restaurants user eats at
88. Kinds of stores user shops at
89. Users who are "receptive" to offers from companies offering online auto insurance, higher education or mortgages, and prepaid debit cards/satellite TV
90. Length of time user has lived in house
91. Users who are likely to move soon
92. Users who are interested in the Olympics, fall football, cricket, or Ramadan
93. Users who travel frequently, for work or pleasure
94. Users who commute to work
95. Types of vacations user tends to go on
96. Users who recently returned from a trip
97. Users who recently used a travel app
98. Users who participate in a timeshare

Anyone think that this is creepy, or worrisome?

Delete your Facebook account

Did you know that a small sample of a hundred plus items that Facebook alone collects about you includes, user income and net worth, user affiliations with credit unions, national banks or regional banks, your preferences in TV shows, users who are "heavy" buyers of beer, wine or spirits, users who are "receptive" to offers from companies offering online auto insurance, higher education or mortgages, and prepaid debit cards/satellite TV?

It is well documented in both books and legislative testimony that the British company Cambridge Analytical turned the military-grade psychological warfare techniques developed to deter ISIS recruitment, against the American voters. These were specifically targeted short-lived Facebook ads used to change opinions and prey on the uninformed and naïve among us. Facebook has been unwilling to this point to share the content of these ads.

In addition, Russian Facebook ads, based on Republican polling data individually targeted Facebook users and spread false narratives to create division among us.

Now for sure, Facebook will track your activities across the Internet even if you do not have a Facebook account. You will need to use web browser extensions like Privacy Badger, Ghostery, and HTTPS Everywhere to block this tracking.

Whatever perceived or real value comes from the use of this social network pales in comparison to the damage caused by fomenting division among us, and to never ever being able to have a free and fair election again in this country. It is now past the time to show your patriotism as an American, and delete your Facebook account, and then continue to protect yourself on the Internet.

1/4/20 Fresh Cambridge Analytica leak 'shows global manipulation is out of control'

Company's work in 68 countries releases more than 100,000 documents

An explosive leak of tens of thousands of documents from the defunct data firm Cambridge Analytica is set to expose the inner workings of the company that collapsed after the Observer revealed it had misappropriated 87 million Facebook profiles.

More than 100,000 documents relating to work in 68 countries that will lay bare the global infrastructure of an operation used to manipulate voters on "an industrial scale" is set to be released over the next months.

It comes as Christopher Steele, the ex-head of MI6's Russia desk and the intelligence expert behind the so-called "Steele dossier" into Trump's relationship with Russia, said that while the company had closed down, the failure to properly punish bad actors meant that the prospects for manipulation of the US election this year were even worse.

https://www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation

Hundreds of Millions of Facebook Users Data Exposed

Information could be deployed for spam or phishing attacks

Information on 267 million Facebook users, including user names, phone numbers and Facebook IDs, was exposed online, according to a cybersecurity researcher.

The data, mostly from U.S. Facebook users, was posted on a searchable database by a group that appeared to be based in Vietnam, said Bob Diachenko, the cyber threat intelligence director at Security Discovery, a Ukrainian cybersecurity website that offers news and consulting services. The Vietnamese group appeared to be charging for access to the data, but a flaw in their code inadvertently left the database open to all, he said.

https://www.bloomberg.com/news/articles/2019-12-20/data-on-hundreds-of-millions-of-u-s-facebook-users-exposed?srnd=technology-vp

Facebook offers funny answer for why it tracks users' locations even when they turn tracking services off

Facebook offered a revealing explanation to lawmakers for why it continues to track users' locations even after those users turn Facebook's location tracking services off.

Responding to a letter from Sen. Josh Hawley, (R-MO), and Sen. Chris Coons, (D-DE), Facebook said it needs that extra location data to target ads, and for various security functions. The two senators asked Facebook last month to "respect" users' decisions to keep their locations private. Coons and Hawley now say that Facebook needs to give users more control over their data. I say, just go ahead and delete Facebook.

https://boingboing.net/2019/12/18/facebook-offers-funny-answer-f.html

1/13/20 Facebook Exec Says Company Helped Elect Trump And May Just Do It Again

Facebook Vice President Andrew Bosworth also said that the president's victory was not a result of outside influence but of clever digital advertising.

Bosworth later shared that the comments were "not meant for public consumption."

Bosworth's December remarks surfaced in reports Tuesday, a day after Trump claimed that Zuckerberg told the president during their dinner in October that he was "number 1" on the social media platform.

https://www.huffpost.com/entry/facebook-exec-company-helped-elect-trump-do-it-again_n_5e154bdcc5b6c7b859d28648

1/23/20

A plea to save Democracy from a reporter

1/24/20

Who's Afraid of the IRS? Not Facebook. (propublica.org)

In March 2008, as Facebook was speeding toward 100 million users and emerging as the next big tech company, it announced an important hire. Sheryl Sandberg was leaving Google to become Facebook's chief operating officer. CEO Mark Zuckerberg, then 23 years old, told The New York Times that Sandberg would take the young company "to the next level." Based on her time at Google, Sandberg soon decided that one area where Facebook was behind its peers was in its tax dodging. "My experience is that by not having a European center and running everything through the US, it is very costly in terms of taxes," she wrote other executives in an April 2008 email, which has not been previously reported. Facebook's head of tax agreed, replying that the company needed to find "a low taxed jurisdiction to park profits." Later that year, Facebook named Dublin as its international headquarters, just as Google had done when Sandberg was there. And just like Google, Facebook concocted an intra-company deal to "park profits" in Ireland, where it would pay a tax rate near zero.

Like its Big Tech peers, Facebook wasn't much afraid of the IRS. But, as it happened, the same year that Facebook started moving profits to Ireland, the IRS launched a team to crack down on deals like that. The effort started aggressively. As we recently reported, the IRS threw everything it had at Microsoft in the largest audit in the agency's history. But shortly after the IRS showed this new ambition, Republicans in Congress, after taking the House in 2010, began forcing cuts to the IRS' budget. Over the years, as Facebook grew into one of the world's largest companies, with 2 billion users, the IRS was shrinking. By the time the IRS finally took on Facebook over its Irish deal a few years later, the agency was in over its head. ProPublica pieced together the story of the Facebook audit from court documents filed by the two sides in their years long battle. The picture revealed by the documents provides a crucial window into the IRS' struggles to check large corporations' tax schemes.

Facebook To Pay $550 Million To Settle Facial Recognition Suit (nbcnews.com)

Facebook has agreed to pay $550 million to settle a class-action lawsuit (Warning: source may be pay walled; alternative source) over its use of facial recognition technology in Illinois, "giving privacy groups a major victory that again raised questions about the social network's data-mining practices," reports The New York Times. From the report: The case stemmed from Facebook's photo-labeling service, Tag Suggestions, which uses face-matching software to suggest the names of people in users' photos. The suit said the Silicon Valley company violated an Illinois biometric privacy law by harvesting facial data for Tag Suggestions from the photos of millions of users in the state without their permission and without telling them, how long the data would be kept. Facebook has said the allegations have no merit. Under the agreement, Facebook will pay $550 million to eligible Illinois users and for the plaintiffs' legal fees.

More reading and viewing:

Meet Brittany Kaiser, Cambridge Analytica Whistleblower Releasing Troves of New Files from Data Firm (six part series)

https://www.democracynow.org/2020/1/7/the_great_-hack_cambridge_analytica

Zucked: Early Facebook Investor Roger McNamee on How the Company Became a Threat to Democracy (four part series)

https://www.democracynow.org/2019/10/23/roger_-mcnamee_zucked_facebook_mark_zuckerberg

Roger McNamee singles out Facebook and Google for their roles in spreading disinformation.

https://finance.yahoo.com/news/roger-mcnamee-on-climate-change-anti-vaxxing-white-supremacy-120859801.html

Facebook Doesn't Know What It Does With Your Data, Or Where It Goes (vice.com) 26

Posted by BeauHD on Wednesday April 27, 2022 @06:00AM from the surprise-surprise dept.

em1ly shares a report from Motherboard: Facebook is facing what it describes internally as a "tsunami" of privacy regulations all over the world, which will force the company to dramatically change how it deals with users' personal data. And the "fundamental" problem, the company admits, is that Facebook has no idea where all of its user data goes, or what it's doing with it, according to a leaked internal document obtained by Motherboard. "We've

built systems with open borders. The result of these open systems and open culture is well described with an analogy: Imagine you hold a bottle of ink in your hand. This bottle of ink is a mixture of all kinds of user data (3PD, 1PD, SCD, Europe, etc.) You pour that ink into a lake of water (our open data systems; our open culture) ... and it flows ... everywhere," the document read. "How do you put that ink back in the bottle? How do you organize it again, such that it only flows to the allowed places in the lake?" (3PD means third-party data; 1PD means first-party data; SCD means sensitive categories data.)

The document was written last year by Facebook privacy engineers on the Ad and Business Product team, whose mission is "to make meaningful connections between people and businesses," and which "sits at the center of our monetization strategy and is the engine that powers Facebook's growth," according to a recent job listing that describes the team. This is the team that is tasked with building and maintaining Facebook's sprawling ads system, the core of the company's business. And in this document, the team is both sounding an alarm, and making a call to change how Facebook deals with users' data to prevent the company from running into trouble with regulators in Europe, the US, India, and other countries that are pushing for more stringent privacy constraints on social media companies. "We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.' And yet, this is exactly what regulators expect us to do, increasing our risk of mistakes and misrepresentation," the document read. In other words, even Facebook's own engineers admit that they are struggling to make sense and keep track of where user data goes once it's inside Facebook's systems, according to the document. This problem inside Facebook is known as "data lineage."

And then as if you haven't already read enough. The reasons given below to use this tool, are the exact same reasons that you should not allow this tool to be used against you and your privacy rights.

Facebook Pixel: What It Is and Why You Need It

If your business advertises on Facebook, you should already know about the Facebook pixel. This code will optimize your Facebook ad strategy and help you make the most of your advertising budget. The Facebook pixel helps you reach new, relevant audiences and track their engagement with your ads.

What Is a Facebook Pixel?

The Facebook pixel is a short piece of code that businesses can add to their website to track their Facebook ad campaigns. The pixel measures ad conversions, website traffic, and monitors audiences.

The Facebook pixel also helps you to create custom audiences for your Facebook ads, allowing you to target certain demographics and retarget customers or visitors to your website.

How Does Facebook Pixel Work?

When a customer takes action on your website, the Facebook pixel code is triggered and reports their actions. The report of your Facebook pixel activity can be found in Facebook's ads manager.

The pixel tracks customer journeys through your website and reveals whether they completed your desired action, whether it's buying a product, subscribing, or filling out a form.

Learning customer data and how they engage with your website and with advertisements can help you focus your target audience, retarget custom audiences, and improve your ads. The Facebook pixel helps you optimize your ads to increase customer conversions.

Facebook Pixel Cost

Installing the Facebook pixel is totally free! Advertising on Facebook is not free, of course, but setting up the Facebook tracking pixel is free. The Facebook pixel will even save you money spent on advertising, as you can get more out of your ads.

Why You Need The Facebook Pixel

The Facebook pixel helps businesses track and optimize their Facebook ads. If you're advertising on Facebook, you should absolutely install the Facebook pixel so that you better understand how your ads perform.

Tracking the Facebook pixel allows you to place your ads in front of the best possible audience, leading to better conversion rates and ROIand ROAS for your ad budget.

Keep reading to learn all the ways that the Facebook pixel can benefit your social media marketing strategy.

https://seodigitalgroup.com/facebook-pixel/

DC Attorney General Sues Mark Zuckerberg Over Cambridge Analytica Data Breach (go.com) 39

Posted by BeauHD on Monday May 23, 2022 @06:00PM from the personally-involved dept.

An anonymous reader quotes a report from ABC News: Washington, D.C., Attorney General Karl Racine has sued Meta CEO Mark Zuckerberg for allegedly failing to protect consumer data following the Cambridge Analytica data leak. "The evidence shows Mr. Zuckerberg was personally involved in Facebook's failure to protect the privacy and data of its users leading directly to the Cambridge Analytica incident," Racine said in a statement about the lawsuit released Monday. "This unprecedented security breach exposed tens of millions of Americans' personal information, and Mr. Zuckerberg's policies enabled a multi-year effort to mislead users about the extent of Facebook's wrongful conduct." He added, "This lawsuit is not only warranted, but necessary, and sends a message that corporate leaders, including CEOs, will be held accountable for their actions."

The lawsuit alleges that Zuckerberg was "responsible for" and "had the clear ability" to control Facebook operations and enabled Cambridge Analytica to use consumer data. The lawsuit alleges that third-party firms like Cambridge Analytica got data from 87 million Americans and half of District of Columbia residents. Racine filed a lawsuit against Facebook in December 2018 for the data leak and is bringing this suit following evidence found during that litigation, according to the attorney general. In March, a judge ruled against an effort by Racine to add Zuckerberg as a defendant in the ongoing 2018 case. [...] The lawsuit filed by Racine takes issue with what it appears to consider a central business objective of Facebook. The suit accuses the company of aiming "to convince people to reveal the most granular details of who they are to Facebook -- their religions, their work histories, their likes -- so that it can be monetized, and Zuckerberg and his company can continue to grow even wealthier." On multiple occasions, the lawsuit notes that the company pursued its policies "at Zuckerberg's direction."

Report: Facebook has Started Encrypting Links to Counter Browsers' Anti-Tracking Measures (ghacks.net) 74

Posted by EditorDavid on Monday July 18, 2022 @07:34AM from the whose-link-is-it-anyway? dept.

"Facebook has started to use a different URL scheme for site links," writes the technology blog Ghacks, "to combat URL stripping technologies that browsers such as Firefox or Brave use to improve privacy and prevent user tracking." Some sites, including Facebook, add parameters to the web address for tracking purposes. These parameters have no functionality that is relevant to the user, but sites rely on them to track users across pages and properties. Mozilla introduced support for URL stripping in Firefox 102, which it launched in June 2022. Firefox removes tracking parameters from web addresses automatically, but only in private browsing mode or when the browser's Tracking Protection feature is set to strict. Firefox users may enable URL stripping in all Firefox modes, but this requires manual configuration. Brave Browser strips known tracking parameters from web addresses as well....

It is no longer possible to remove the tracking part of the URL, as Facebook merged it with part of the required web address.

Zuckerberg and Sandberg Ordered To Testify Over Alleged Involvement In Cambridge Analytica Scandal (gizmodo.com) 23

Posted by BeauHD on Wednesday July 20, 2022 @11:30PM from the time-to-face-the-music dept.

An anonymous reader quotes a report from Gizmodo: Meta CEO Mark Zuckerberg and former COO Sheryl Sandberg will have to provide testimony to a federal court to discuss their alleged involvement in the company's notorious Cambridge Analytica scandal, over half a decade since it first captured the world's attention. [...] Cambridge Analytica was a British political consulting firm that used Facebook user data to target and lobby potential voters ahead of the 2016 election in favor of Donald Trump. The ensuing scandal helped trigger an investigation from the Federal Trade Commission that resulted in Facebook agreeing to a record-setting $5 billion settlement over its privacy practices.

A new filing (PDF) in the Northern District of California Tuesday shows Zuckerberg and Sandberg agreed to be deposed for six and five hours respectively in September of this year. This comes as part of a class action lawsuit filed against Meta, claiming the company violated consumer privacy laws when it shared user data with Cambridge Analytica back in 2015. [...] In addition to Zuckerberg and Sandberg, the court's also seeking to depose Meta's newly named CTO Javier Olivan -- who previously served as the company's Chief Growth Officer -- as well as a handful of other "key witnesses." Olivan's deposition is expected to last three hours. According to Tuesday's filing Meta will also hand over 1,200 documents "previously withheld as privileged." Plaintiffs in the case previously accused Meta and the law firm representing it of "stonewalling," during the court's discovery phase.

Stop using Google

The Internet was purposely designed with its intelligence, like personal computers and other connecting devices, only at the end points. More specifically, it was designed as a democratic system with no centralized computer control of access, or data collection. This design was mostly a reaction to the perceived centralized fascistic operation of the prior mainframe computer era and its dumb terminals for computer users.

But now these unbridled capitalist digital gangster corporations like Google, have inserted themselves as Internet gateways into every transaction and communication across your Internet. They have, without your express permission, exerted Eminent Domain over your personal data. They refer to this data as digital exhaust, a euphemism to obfuscate and diminish this theft. Google alone (10 million servers headed for 100 million) collects a staggering amount of data and stores it forever. More than 500 megabytes per person **per day**. By way of comparison, this letter as an MS Word document equals about 0.3% of that amount of daily collected personal data.

4.62 billion pages indexed by Google as of May 2016, according to WorldWideWebSize
Almost 148 million domains or unique websites, as estimated by DomainTools
More than 3.5 billion Google searches covering more than 20 billion sites every day, as reported by Internet Live Stats

New York (CNN Business) Google has confirmed its collecting health data on millions of Americans through a new partnership with Ascension, one of the country's largest nonprofit health systems. The project is codenamed "Project Nightingale," although this revelation is light on specifics, Google and Ascension said the partnership would integrate Ascension's various silos of health data into the cloud. (In other words, Googles server computers)

Imaging how this data might be used against you in the future, for insurance applications, college admissions, life insurance applications, or employment applications. Think of the effect not only on you, but your children and grandchildren.

Not unlike the Truman show movie, Google is using their tools and code to record everyone's digital lives, monitoring, guiding, predicting behaviors, and make enormous profits from doing this.

What to do? Stop giving them your personal data! Use DuckDuckGo or better yet StartPage, for a search engine that does not track you. Use browser extensions to block ads and tracking your browsing history, and use Private Browsing.

Stop using the Google Chrome browser because it tracks you, the Mozilla Firefox browser does not. Do not buy or use a Chromebook, it is a surveillance tool. Do not use Alexa for the same reason. Stop using Google Docs and use Libre Office or MS Office instead. Do not use Google Maps or YouTube. Use openstreetmap.org and Vimeo.com instead. I know you like cat videos, but do it anyway. Do not use a Ring doorbell either, or other Internet connected cameras, appliances, thermostats, and baby monitors.

Amazon is facing criticism over its home security cameras called Ring, after a data leak exposed the personal information of over 3,000 users. The data breach includes emails, passwords and other sensitive information that would allow hackers to access live camera footage from inside every room of people's homes. The data breach follows criticism over Ring's cooperation with more than 400 police departments, giving cops the ability to use homeowners' camera footage in their investigations. A group of 30 civil rights groups published a joint letter demanding that lawmakers stop the police partnership, calling it a threat to civil rights and liberties, especially for black and brown communities.

https://www.democracynow.org

Corporate abuse can be stopped, as were the 19th-century Robber Barons. Government intervention filed an antitrust case against IBM in the 1970's, broke up AT&T in the 1980's, throttled Microsoft with a consent decree in the 1990's , and fined Facebook and Google millions of dollars numerous times in the 2000's.

You should advocate for enforcement of existing laws, (Sherman Antitrust Act) and for creating data protection laws like those enacted in the European Union.

The "Don't be Evil" slogan of an early benevolent startup company has been replaced by a malevolent software industry monopolist, because of all the money they can make from you.

To quote whistleblower Ed Snowden, "I don't want to live in a world where everything that I say, everything I do, every thought, every aspiration, everyone I talk to, every expression of creativity or love or friendship is recorded and stored permanently."

Remember, there is no cloud. That is just another corporate euphuism for other people's computers (servers). In the cloud your personal information is not yours, but theirs.

They cannot be trusted, as they have a proven history of not being able to protect your data, and of using it in personally detrimental ways. You have everything to lose.

https://firewalltimes.com/recent-data-breaches/

The monopolist claim that data (your personal information) is like the new oil. They are leaking it everywhere.

Google Ordered Russian Translators Not to Call War in Ukraine a War

Internal email shows that despite its anti-war stance, the company bowed to Kremlin decrees.

https://theintercept.com/2022/03/28/google-russia-ukraine-war-censorship/

Google Issues Third Emergency Fix for Chrome This Year (theregister.com) 23

Posted by msmash on Friday April 15, 2022 @02:45PM from the security-woes dept.

Google is issuing fixes for two vulnerabilities in its Chrome web browser, including one flaw that is already being exploited in the wild. From a report: The emergency updates the company issued this week impact the almost 3 billion users of its Chrome browser as well as those using other Chromium-based browsers, such as Microsoft Edge, Brave and Vivaldi. It is the third such emergency update Google has had to issue for Chrome this year. One of the flaws is a type confusion vulnerability tracked as CVE-2022-1364, a high-severity, zero-day bug that is actively being used by attackers. With a type confusion flaw, a program will allocate a resource like a pointer or object using one type but later will access the resource using another, incompatible type. In some languages, like C and C++, the vulnerability can result in out-of-bounds memory access. This incompatibility can cause a browser to crash or trigger logical errors. However, if exploited, it could enable a hacker to execute arbitrary code.

Documents Reveal Advanced AI Tools Google Is Selling to Israel

Google employees, who have been kept in the dark about the "Nimbus" AI project, have concerns about Israeli human rights abuses.

https://theintercept.com/2022/07/24/google-israel-artificial-intelligence-project-nimbus/

Stop Using Amazon

I know, I know, this is a hard one for me to write as well.

I have never purchased anything at a Walmart store, in part because they treat their employees badly; put two people out of work for everyone they hire, and love to suck off the government corporate welfare teat. They have put some of my favorite business out of business where I have lived. Wolahan's in

for good lumber, Thrifty Mac's for any hardware you can imagine, K-Mart for underwear.

Now it is the same for Amazon

Treat employees badly, and have a large carbon footprint.

Digital command, robots into action, persons picking, airplanes, trucks etc. just get something simple to me.

Reduced inventory at home improvement stores. It is frustrating to shop these days at grocery stores and home improvement stores.

I went to Lowe's looking for some gutter slash guards and they did not have any. Then I went to Menards and they had some, but only in white for my brown gutters. They had lots of brown gutter pipes and elbows but no brown screws. How many of these parts are they going to sell without brown screws? So what to do? Shop Amazon.com, and put my digital commands into their datacenters, putting robots into action, persons picking, airplanes loading, trucks delivering etc. just to get something simple to me. I could feel my carbon footprint expanding.

Simply things are no longer available in grocery stores either. Want some particular soap or shampoo you have been buying for years or decades. They do not have it. They have hundreds of different odd Generation X, Y, and Z brands, but not basic simple stuff.

It is like going to buy a potato and only being able to get a twice-baked, sour cream and onion with chives variety.

What to do? Shop Amazon.com, and put my digital commands into their datacenters, putting robots into action, persons picking, airplanes loading, trucks delivering etc.

Sure, you have to buy a case of soap or shampoo, but I still buy green bananas as well.

Ring Ukraine News Suppressed at Amazon's Request, Journalists Say

https://theintercept.com/2020/01/24/amazon-ring-ukraine/

I Want You Back: Getting My Personal Data From Amazon Was Weeks of Confusion and Tedium

I asked Amazon to provide the data it had collected on me. The process was a labyrinthine endurance test.

https://theintercept.com/2022/03/27/amazon-personal-data-request-dark-pattern/

Broadband Internet for All

As background to this piece, I have spent much of my adult life working to bridge the Digital Divide of access to computers and Internet service. I did this by refurbishing many thousands of corporate surplus computers for use by schools, nonprofits, and low-income families. And by running a low cost dial in phone line Internet service to provide Internet access for many hundreds of families, and connect them to the Internet via a wireless broadband connection from a local ISP, and later with a DSL connection from a telecom provider.

But first a bit of more relevant history.

History is clear in that without a massive public investment, there would be no Internet. It is also clear that we now need a broadband plan would take the first steps towards returning the Internet to its rightful owners, the public. This will ensure that everyone can have reliable, high-speed broadband.

Right now, nearly half of Americans do not have an Internet connection that meets minimum broadband speeds. Moreover, a staggering number of poor people of color do not have home Internet access of any kind. Yet Americans are charged some of the highest prices for Internet service in the developed world. These are all symptoms of a much larger, structural problem: the corporate capture of the pipes, wires, and other infrastructure that powers the Internet.

H.R.3152 - Rural Broadband Initiative Act 114th Congress (2015-2016)

To amend the Rural Electrification Act of 1936 to establish an Office of Rural Broadband Initiatives in the Department of Agriculture because the Rural Electrification Act of 1936 helped bring electricity and telephone service to rural America, thus removing major barriers to the development of our rural economies. A lack of affordable broadband presents a similar barrier to the development of our rural economy. According to the FCC, 53 percent of rural Americans lack access to service delivering broadband speeds of 25 Mbps for downloads and 3 Mbps for uploads. High-speed broadband access helps rural communities compete and grow in our digital economy. **Died in Congress.** Legislation not enacted in the current session of Congress is forever cleared from the books.

Wisconsin Rural Broadband Efforts Largely Unnoticeable

In its first two years, the program has benefited just a few thousand households served by 14 Wisconsin service providers. Efforts to bridge rural broadband disparities fall well short of a solution for most outside of urban areas, according to Internet service providers and industry experts.

https://www.govtech.com/network/Wisconsin-Rural-Broadband-Efforts-Largely-Unnoticeable-.html

Despite billions of public dollars, some rural residents slog through slow Internet

A spokeswoman for Madison-based TDS Telecom said it is difficult to say whether TDS would have expanded broadband service to rural areas without federal dollars.

https://madison.com/wsj/business/despite-billions-of-public-dollars-some-rural-residents-slog-through/article_a6d5f951-7937-5e37-b7dc-54b5fd88460c.html

TDS Telecom for example is currently in the process of providing upgraded fiber backbone to Wisconsin via the current Federal Rural Broadband Initiative. The plan covers the Madison and Wausau suburbs mostly in the central and western parts of the state, the least rural areas. This leaves the northeastern area out of luck, and gives our rural communities the choice of spotty cable service, slow expensive cellular service, or slow and even more expensive satellite service. https://tdsfiber.com/build/ Sorry zip code 54214, no fiber for you! Except for the "fiber to the telecom press releases," we continue to see over and over for many decades now.

For many years, Broadband Internet supporters have attempted to reconcile the public interest in universal, high-quality broadband against the profit motives of Internet Service Providers (ISPs). They tried to tame their malfeasance but not break them up and leave their ownership and control of the Internet infrastructure intact.

It has now become clear that they are in fact responsible for the sorry state of broadband in this country, having received $400 Billion in subsidies and discounts over the past century that they have not lived up to. We should now make them pay us back to fix it. The Book of Broken Promises

http://teletruth.org/

See also: America's Broadband Heroes: Fixed Wireless Broadband Providers www.wispa.org.

It is now well past the time to develop a vision of what a more democratic communication system that operates outside of the existing market would look like.

Some current presidential candidates have unveiled plans to create publicly owned broadband Internet networks as an expansion of, and eventual replacement for, the existing system. These plans create public interest regulations on existing ISP's,

using antitrust legislation much as we currently regulate the companies that manage electricity, gas, and other critical infrastructure utilities in the United States. Most importantly, the plans would create publicly owned competitive alternatives to corporate ISPs.

It Now Seems as if Another Internet Connection Method is Actually Possible

Over the past 20 years across the country, hundreds of cities and towns have taken it upon themselves to build their own publicly owned broadband networks. In general, these networks are cheaper, faster, and operate with greater public accountability, despite lacking their enormous economies of scale. Despite having been fought against tooth and nail by the incumbent ISP's. https://muninetworks.org/

Current proposed High-Speed Internet for All plans provide Federal support for local broadband initiatives, or Internet cooperatives. The plans propose billions in infrastructure grants to be distributed to municipalities and states that want to voluntarily build out publicly owned and democratically controlled co-operative, open access broadband networks.

These plans do not build broadband infrastructure, but make the political terrain more tolerant of the expansion of public broadband initiatives. This is done by providing funding and technical assistance, and repealing laws in twenty-five states that prohibit or inhibit municipalities from building their own networks.

These public broadband networks would invest in low-income neighborhoods and would be required to abide by universal service requirements. These networks would be required to deploy technologies that meet minimum speed thresholds, and would condition grants on and adherence to strong labor, wage, and sourcing standards.

The funding sources for all of this new democracy are unclear at this point, but hey, how about we get some of that $400 billion back? Perhaps a tax or a rebate in exchange for no prison time for the fraud and extortion carried out against all of us.

Under these plans, the FCC would be de-neutered and be again able to regulate the rates that for-profit ISPs can charge their subscribers. ISPs would also be required to offer a low-cost Internet plan, which would be fully subsidized by the government for low-income households. Eligibility for subsidized Internet access would be tied to eligibility for means-tested social programs like SNAP and Medicaid, effectively integrating Internet access into the welfare state. This would put more money back in the hands of low-income families, and help close America's cavernous digital divide. Internet for All would also provide a source of jobs to construct and maintain the network. Installing high-speed Internet could also potentially attract greater capital investment.

We could have a "public option" for Internet service that brings competing services to everyone regardless of his or her city, state, or zip code. After all, the Internet was invented from a massive public investment. It should now be returned to its rightful owners.

Source info: *https://www.jacobinmag.com/2019/12/broadband-Internet-bernie-sanders*

So in the end, Rural Broadband service equals economic growth, by keeping Wisconsin's talented young people from leaving the rural areas of the state and not limiting their ability to thrive in a digital economy. As of 2017, US ranks 9th in the world in fixed broadband speed at 70.75 Mbps average, but this is less than half top-ranked Singapore's 154.38 Mbps. The US is also one of the most expensive nations: in 120th place (out of 195).with an average monthly cost of $67.69. Locally, Wisconsin ranks 41st in the United States in its ranking for Internet access, 32nd for broadband access with an average speed of 37.4 Mbps and coverage of 85.3%.

"In July 2013, the state created the Broadband Expansion Grant program to help meet the demand for improved broadband and encourage its development in Wisconsin's unserved and underserved areas. Since then, the PSC has awarded approximately $20.1 million to 138 grant projects over six years. In September 2019, the PSC opened the Broadband Expansion Grant applications for 2020. This grant cycle provides up to $24 million for improving Internet access across Wisconsin."

https://psc.wi.gov/Pages/Programs/WBO.aspx

This appears to be just enough money to say you did something, but not really.

"With the development of the Internet we are in the middle of the most transforming technological event since the capture of fire. I used to think that it was just the biggest thing since the Gutenberg printing press, but now I think you have to go back further." *John Perry Barlow*

Free the Internet

First, a bit of history. The first version of the Internet was born as a science project of the Advanced Research Projects Agency of the United States Department of Defense. ARPANET as it was known in the late 1960s, was developed primarily for military use, and was funded mainly by US Government National Science Foundation (NSF) grant monies. At the time, Senator Al Gore Jr. from Tennessee, was a visionary on this subject, and thus was instrumental in advocating for this funding. The ARPANET was fundamentally about linking static read-only scientific and academic materials together; to assist the DOD with advanced forward thinking research much of it being conducted at universities all around the country.

The second version of the Internet came around 1995 when this primarily scientific and academic network was opened to the public and the control and management of it turned over to a nonprofit organization called IETF. The Internet Engineering Task Force is an open standards international membership-based non-profit organization, which develops and promotes voluntary Internet standards. The Internet founders, including Tim Berners-Lee, also formed WW3, the World Wide Web Consortium as a standards body. It is interesting to note that Berners-Lee basically invented the web and then turned it over to the world.

As a reflection of humble beginnings, for the first 20 years domain registration was handled by one guy, Jon Postel. Then they formed ICANN, The Internet Corporation for Assigned Names and Numbers. It is responsible for coordinating the maintenance and procedures the databases related to the namespaces and numerical spaces of the Internet, (called DNS) ensuring the network's stable and secure operation. They also started charging for registering domain names. The Internet remained in a beta (developmental) stage, being originally developed and designed for sharing of information by people based on an idealistic honor system. This then further developed into a linked data semantic web with the development of a browser, funded with grant money by guess who? The NSF, again.

When corporations started driving the WW3 is where things started to go wrong. This is when the original decentralization standard was murdered and corporations started to seize control

and enact its perverted vision of Manifest Destiny over the data of citizens worldwide. The founders believed that the Internet/Web was about augmenting our collective intelligence as a species. A fight has been raging to overcome this evil ever since, despite the oversized egos of the builder hackers, and to bring decentralized identity verification for financial transactions and social media applications to the Web.

This pubic opening also led to the incubation of many startup companies driving ecommerce, the expansion of access to human knowledge, the proliferation of both digital music and cat video's, as well as tremendous economic and social growth. This second version was fundamentally about being interactive for read and write and for linking to programs which by the 2000's had evolved to include social media, and a large number of new businesses.

Those of us who enjoyed this phase during the 1990's now look back fondly at how joyful this experience was, even on a 56k or slower dialup connection, or 256k slow broadband connection. We now look back ashamedly at how single mindedly technically focused, and naïve we were about the dirty world around us.

Back in the 1990's no one had worried about all the disparate data being collected by the earlier computers, because we thought we knew there would never be a way to aggregate it all these disparate databases into anything useful to anyone. We were all wrong, very, very, horribly wrong.

The unregulated profit incentives birthed server farms, and Internet clouds, web crawlers, bots, and the algorithms to find, manipulate, and sort the big data of first a nation, and then the entire planet. These corporations have now built these dystopian parasitic surveillance machines, which prey on the entire human species.

Millions and then billions of simple minded and uninformed humans acted like oblivious lemmings all stepping off digital cliffs and into the corporate clouds. Their personal data is vacuumed like some giant digital spider spinning its web to entrap them and then sucking dry anything that smells like personal data from the transfer pipes containing the digital lives of billions of people on the planet.

Corporations profited from and used this data harvested through this predatory surveillance capitalism to alter the thinking, habits, purchases, and voting preferences of the masses in the now damaged and failing democracies. Yet these lemmings continued to carry these tracking devices with them

and placed additional dystopian surveillance machine devices in their homes, on their homes, and in their cars, being misled by some misguided sense of convenience. They did this of course, because their connected parasitic devices told them to.

Those around the world now impoverished, unemployed and without hope from being on the wrong end of Western Empire building, became criminals to survive and who seek out your money with phishing emails for malware and ransomware attacks on your computers.

Hacking is now persistent and accelerating in the number of ransomware, spyware, malware, and other computer intrusions and infections. This is due most of the entire world being able to access the Internet and those with bad intent able to scan the globe for individual computer weaknesses. It no longer matters if you are an individual, a small business, or a large one. You will be targeted if a weakness is spotted, regardless.

And of course, the American National Security Agency or NSA is hovering up all worldwide digital communications under the guise of Signals Intelligence (SISINT). Using their significant computer power to translate all of these zeros and ones into Human Intelligence (HUMINT) to know everything about everyone. "Collect it all," they said. They are storing all of this data on a server farm in Utah… forever.

So obviously based on the current rate of hacking of systems, resulting data breeches, and data collection, we know our software tools in use now are badly broken. People are being harmed, and some would go even further to say robbed, enslaved, and terrorized. I dread the day when some mad genius applies Artificial Intelligence (AI) to these hacking tools and fundamentally kills the Internet, as we know it. Perhaps we will all then need to hide out on the Dark Web, although the TOR browser has its own problems with metadata leakage and with NSA monitoring of the entry and exit nodes.

"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one does not want the whole world to know, but a secret matter is something one does not want anybody to know. Privacy is the power to selectively reveal oneself to the world." Eric Hughes, 1993

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask those of you from the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather." — John Perry Barlow, "A Declaration of the Independence of Cyberspace" February, 1996

https://www.eff.org/cyberspace-independence

Yet the very insecure idealistic open architecture of the Internet web is what prevents privacy today, but every once in a while the good guys win one.

California Net Neutrality Law To Remain Intact After Appeals Court Says It Won't Reconsider Earlier Decision (theverge.com) 14

Posted by msmash on Thursday April 21, 2022 @04:08PM from the moving-forward dept.

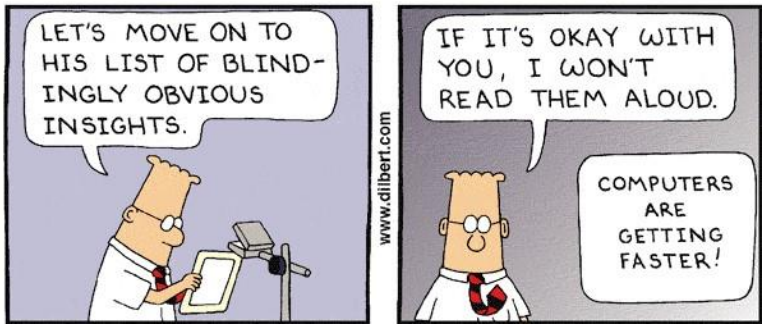
A federal appeals court has denied a request for a rehearing on its January decision that upholds California's net neutrality law. From a report: The 2018 law, widely considered the strongest in the US, was signed into law a year after the Federal Communications Commission (FCC) repealed the Open Internet Order. That order had established stringent net neutrality rules that prohibited internet service providers from throttling or blocking legal websites and apps, and banned ISPs from prioritizing paid content. California's law, which finally took effect last year, also prohibits throttling and speed lanes. Wireless trade associations including the NCTA, the CTIA, and ISPs including Comcast, Verizon, and AT&T sued to block California's law from taking effect, saying the FCC decision should preempt the state law. But that challenge was rejected by a district court judge.

The Ninth Circuit voted 3-0 in January to uphold the lower court ruling, saying the FCC "no longer has the authority" to regulate broadband internet services because the agency reclassified them as "information services, instead of telecommunications services. The FCC therefore cannot preempt the state action." FCC chairwoman Jessica Rosenworcel praised the decision on Twitter, reiterating her position that she wants to see net neutrality become "the law on the land" again. The FCC can't currently reinstate net neutrality at the federal level however since the panel lacks a majority and the two Democrats and two Republicans remain deadlocked on the issue. President Biden's FCC nominee Gigi Sohn is still awaiting a confirmation vote in the Senate.

A Clear and Transparent Digital Bill of Rights

1. A customer must consent or opt in when personal information is collected or shared with a third party and must be able to limit the use of information not required to provide the requested service.
2. A customer must be able to obtain, edit, and delete personal information held by a vendor.
3. A customer must be notified immediately when the security of this information is breeched.
4. A customer must be able to move his/her collected information in a conveniently useable and machine-readable format.

HOW CAN WE REBUILD THE TRUST OF OUR CUSTOMERS? LET'S BRAINSTORM.
Trust
WE COULD STOP USING MISLEADING BENCH-MARK TESTS TO SELL SHODDY PRODUCTS THAT HAVE HIDDEN COSTS.
I HEARD SOMEONE SAY "LIE." LET'S WRITE THAT ONE DOWN.
Trust
DilbertCartoonist@gmail.com
Dilbert.com
10-15-10 © 2010 Scott Adams, Inc./Dist. by UFS, Inc.


LET'S MOVE ON TO HIS LIST OF BLIND-INGLY OBVIOUS INSIGHTS.
www.dilbert.com
IF IT'S OKAY WITH YOU, I WON'T READ THEM ALOUD.
COMPUTERS ARE GETTING FASTER!

What is considered personal data under the EU GDPR?

The European Union's General Data Protection Regulation (GDPR) tries to strike a balance between being strong enough to give individuals clear and tangible protection while being flexible enough to allow for the legitimate interests of businesses and the public. As part of this balancing act, the GDPR goes to great lengths to define what is and is not personal data.

https://gdpr.eu/eu-gdpr-personal-data/

EU agrees rules to force big tech to rein in illegal content or face huge fines

Digital Services Act can now fine platforms like Facebook, Google and Twitter up to 6% of their global revenue

Large online platforms including Facebook, Google and Twitter will have to do more to tackle illegal content or face multibillion euro fines under a new European Union regulatory regime agreed on Saturday.

The wide-ranging Digital Services Act (DSA) can fine a company up to 6% of its global turnover for violating the rules – which would be $7bn (£5.9bn) in the case of Facebook's owner – while repeated breaches could result in a tech firm being banned from doing business in the EU.

https://www.theguardian.com/world/2022/apr/23/eu-agrees-rules-to-force-big-tech-to-rein-in-content-or-face-huge-fines

Hopefully now by the end of this book, you are a lot more knowledgeable and capable of keeping:

In the words of Julian Assange, *"Keep Calm and Encrypt."*

The Hacker Manifesto

By

+++The Mentor+++

Written January 8, 1986

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...

Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's techno brain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my world...

Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...

Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."

Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me... Or feels threatened by me.. Or thinks I'm a smart ass.. Or doesn't like teaching and shouldn't be here...

Damn kid. All he does is play games. They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetency is sought... a board is found. "This is it... this is where I belong..." I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...

Damn kid. Tying up the phone line again. They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those

few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

A Cypherpunks Manifesto

by Eric Hughes

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

If two parties have some sort of dealings, then each has a memory of their interaction. Each party can speak about their own memory of this; how could anyone prevent it? One could pass laws against it, but the freedom of speech, even more than privacy, is fundamental to an open society; we seek not to restrict any speech at all. If many parties speak together in the same forum, each can speak to all the others and aggregate together knowledge about individuals and other parties. The power of electronic communications has enabled such group speech, and it will not go away merely because we might want it to.

Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. Since any information can be spoken of, we must ensure that we reveal as little as possible. In most cases personal identity is not salient. When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others are saying to me; my provider only need know how to get the message there and how much I owe them in fees. When my identity is revealed

by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must always reveal myself.

Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.

Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available to the world, I have no privacy. To encrypt is to indicate the desire for privacy, and to encrypt with weak cryptography is to indicate not too much desire for privacy. Furthermore, to reveal one's identity with assurance when the default is anonymity requires the cryptographic signature.

We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak. To try to prevent their speech is to fight against the realities of information. Information does not just want to be free, it longs to be free. Information expands to fill the available storage space. Information is Rumor's younger, stronger cousin; Information is fleeter of foot, has more eyes, knows more, and understands less than Rumor.

We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do.

We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.

Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide. We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down.

Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation's border and the arm of its violence. Cryptography will ineluctably spread over the whole globe, and with it the anonymous transactions systems that it makes possible.

For privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Privacy only extends so far as the cooperation of one's fellows in society. We the Cypherpunks seek your questions and your concerns and hope we may engage you so that we do not deceive ourselves. We will not, however, be moved out of our course because some may disagree with our goals.

The Cypherpunks are actively engaged in making the networks safer for privacy. Let us proceed together apace.

Onward.

Eric Hughes

9 March 1993

The Crypto Anarchist Manifesto

From: tcmay@netcom.com (Timothy C. May)
Subject: The Crypto Anarchist Manifesto
Date: Sun, 22 Nov 92 12:11:24 PST

Cypherpunks of the World,

Several of you at the "physical Cypherpunks" gathering yesterday in Silicon Valley requested that more of the material passed out in meetings be available electronically to the entire readership of the Cypherpunks list, spooks, eavesdroppers, and all. <Gulp>

Here's the "Crypto Anarchist Manifesto" I read at the September 1992 founding meeting. It dates back to mid-1988 and was distributed to some like-minded techno-anarchists at the "Crypto '88" conference and then again at the "Hackers Conference" that year. I later gave talks at Hackers on this in 1989 and 1990.

There are a few things I'd change, but for historical reasons I'll just leave it as is. Some of the terms may be unfamiliar to you...I hope the Crypto Glossary I just distributed will help.

(This should explain all those cryptic terms in my .signature!)

--Tim May

A specter is haunting the modern world, the specter of crypto anarchy.

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re-routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.

The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade. The methods are based upon public-key encryption, zero-

knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. The focus has until now been on academic conferences in Europe and the U.S., conferences monitored closely by the National Security Agency. But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable. And the next ten years will bring enough additional speed to make the ideas economically feasible and essentially unstoppable. High-speed networks, ISDN, tamper-proof boxes, smart cards, satellites, Ku-band transmitters, multi-MIPS personal computers, and encryption chips now under development will be some of the enabling technologies.

The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.

Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property.

Arise, you have nothing to lose but your barbed wire fences!

Timothy C. May tcmay@netcom.com

THE CYPHERNOMICON

1. Introduction

1.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved.

See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

1.2. Foreword

- The Cypherpunks have existed since September, 1992. In that time, a vast amount has been written on cryptography, key escrow, Clipper, the Net, the Information Superhighway, cyber terrorists, and crypto anarchy. We have found ourselves (or

placed ourselves) at the center of the storm.

- This FAQ may help to fill in some gaps about what we're about, what motivates us, and where we're going. And maybe some useful knowledge on crypto, remailers, anonymity, digital cash, and other interesting things.

+ The Basic Issues

+ Great Divide: privacy vs. compliance with laws

+ free speech and privacy, even if means some criminals cannot be caught (a stand the U.S. Constitution was strongly in favor of, at one time)

- a man's home is his castle...the essence of the Magna Carta systems...rights of the individual to be secure from random searches

+ or invasive tactics to catch criminals, regulate behavior, and control the population

- the legitimate needs to enforce laws, to respond to

situations

+ this parallels the issue of self-protection vs. protection by law and police

- as seen in the gun debate

- crypto = guns in the sense of being an individual's

preemptive protection

- past the point of no return

- Strong crypto as building material for a new age

+ Transnationalism and Increased Degrees of Freedom

- governments can't hope to control movements and communications of citizens; borders are transparent

+ Not all list members share all views

- This is not "the Official Cypherpunks FAQ." No such thing can exist. This is the FAQ I wanted written. Views expressed are my own, with as much input from others, as much consensus, as I can manage. If you want a radically different FAQ, write it yourself. If you don't like this FAQ, don't read it. And tell your friends not to read it. But don't bog down my mailbox, or the 500 others on the

list, with messages about how you would have worded Section 12.4.7.2 slightly differently, or how Section 6.9.12 does not fully reflect your views. For obvious reasons.

- All FAQs are the products of a primary author, sometimes of a committee. For this FAQ, I am the sole author. At least of the version you are reading now. Future versions may have more input from others, though this makes me nervous

(I favor new authors writing their own stuff, or using hypertext links, rather than taking my basic writing and attaching their name to it--it is true that I include the quotes of many folks here, but I do so by explicitly quoting them in the chunk they wrote....it will be tough for later authors to clearly mark what Tim May wrote without excessively cluttering the text. The revisionist's dilemma.

- The list has a lot of radical libertarians, some anarcho- capitalists, and even a few socialists

- Mostly computer-related folks, as might be expected. (There are some political scientists, classical scholars, etc. Even a few current or ex-lawyers.)

For the remaining almost 400 pages of this early Internet FAQ, see one of these sites:

https://nakamotoinstitute.org/static/docs/cyphernomicon.txt

https://www.tcw.org/lefty/Short%20Stories/THE%-20CYPHERNOMICON.pdf

A Declaration of the Independence of Cyberspace

by John Perry Barlow

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.

You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.

You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real

conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.

Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.

In the United States, you have today created a law, the Telecommunications Reform Act, which repudiates your own Constitution and insults the dreams of Jefferson, Washington, Mill, Madison, DeToqueville, and Brandeis. These dreams must now be born anew in us.

You are terrified of your own children, since they are natives in a world where you will always be immigrants. Because you fear them, you entrust your bureaucracies with the parental responsibilities you are too cowardly to confront yourselves. In our world, all the sentiments and expressions of humanity, from the debasing to the angelic, are parts of a seamless whole, the global conversation of bits. We cannot separate the air that chokes from the air upon which wings beat.

In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace. These may keep out the contagion for a small time, but they will not work in a world that will soon be blanketed in bit-bearing media.

Your increasingly obsolete information industries would perpetuate themselves by proposing laws, in America and elsewhere, that claim to own speech itself throughout the world. These laws would declare ideas to be another industrial product, no more noble than pig iron. In our world, whatever the human mind may create can be reproduced and distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish.

These increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers. We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.

We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.

Davos, Switzerland February 8, 1996

Guerilla Open Access Manifesto

Information is power. But like all power, there are those who want to keep it for themselves. The world's entire scientific and cultural heritage, published over centuries in books and journals, is increasingly being digitized and locked up by a handful of private corporations. Want to read the papers featuring the most famous results of the sciences? You'll need to send enormous amounts to publishers like Reed Elsevier.

There are those struggling to change this. The Open Access Movement has fought valiantly to ensure that scientists do not sign their copyrights away but instead ensure their work is published on the Internet, under terms that allow anyone to access it. But even under the best scenarios, their work will only apply to things published in the future.

Everything up until now will have been lost.

That is too high a price to pay. Forcing academics to pay money to read the work of their colleagues? Scanning entire libraries but only allowing the folks at Google to read them?

Providing scientific articles to those at elite universities in the First World, but not to children in the Global South? It's outrageous and unacceptable.

"I agree," many say, "but what can we do? The companies hold the copyrights, they make enormous amounts of money by charging for access, and it's perfectly legal — there's nothing we can do to stop them." But there is something we can, something that's already being done: we can fight back.

Those with access to these resources — students, librarians, scientists — you have been given a privilege. You get to feed at this banquet of knowledge while the rest of the world is locked out. But you need not — indeed, morally, you cannot — keep this privilege for yourselves. You

have a duty to share it with the world. And you have: trading passwords with colleagues, filling download requests for friends.

Meanwhile, those who have been locked out are not standing idly by. You have been sneaking through holes and climbing over fences, liberating the information locked up by the publishers and sharing them with your friends.

But all of this action goes on in the dark, hidden underground. It's called stealing or piracy, as if sharing a wealth of knowledge were the moral equivalent of plundering a ship and murdering its crew. But sharing isn't immoral — it's a moral imperative. Only those blinded by greed would refuse to let a friend make a copy.

Large corporations, of course, are blinded by greed. The laws under which they operate require it — their shareholders would revolt at anything less. And the politicians they have bought off back them, passing laws giving them the exclusive power to decide who can make copies.

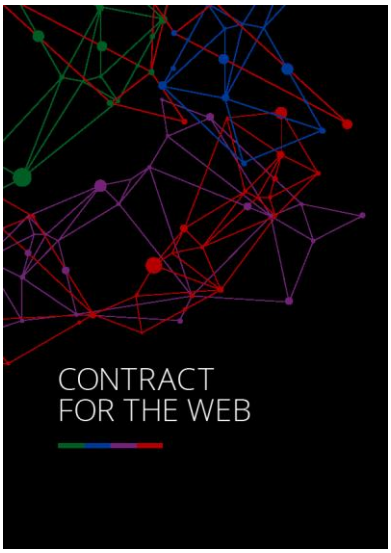
There is no justice in following unjust laws. It's time to come into the light and, in the grand tradition of civil disobedience, declare our opposition to this private theft of public culture.

We need to take information, wherever it is stored, make our copies and share them with the world. We need to take stuff that's out of copyright and add it to the archive. We need to buy secret databases and put them on the Web. We need to download scientific journals and upload them to file sharing networks. We need to fight for Guerilla Open Access.

With enough of us, around the world, we'll not just send a strong message opposing the privatization of knowledge — we'll make it a thing of the past. Will you join us?

Aaron Swartz
July 2008, Eremo, Italy

Contract-for-the-Web



Contract for the Web-Principles

PRINCIPLE 1

Governments will Ensure everyone can connect to the internet So that anyone, no matter who they are or where they live, can participate actively online

PRINCIPLE 2

Keep all of the Internet available, all of the time so that no one is denied their right to full internet access

PRINCIPLE 3

Respect and protect people's fundamental online privacy and data rights so everyone can use the Web freely, safely and without fear

PRINCIPLE 4

Make the internet affordable and accessible to everyone so that no one is excluded from using and shaping the web

PRINCIPLE 5

Respect and protect people's privacy, personal data, and other online data rights to build online trust so people are in control of their lives online, empowered with clear and meaningful choices around their data and privacy

PRINCIPLE 6

Companies will develop technologies that support the best in humanity and challenge the worst so the web really is a public good that puts people first

PRINCIPLE 7

Citizens will be creators and collaborators on the web so the web has rich and relevant content for everyone

PRINCIPLE 8

Citizens will build strong communities that respect civil discourse and human dignity so that everyone feels safe and welcome online

PRINCIPLE 9

Citizens will fight for the web so the web remains open and a global public resource for people everywhere, now and in the future

Download the PDF https://contractfortheweb.org/

Declaration-for-the-Future-for-the-Internet

The White House issued a 'Declaration for the Future of the Internet ' on April 28, 2022, in partnership with 60 other nations and global accords, which outlined the United States' agenda for the Internet under President Joe Biden.

We are united by a belief in the potential of digital technologies to promote connectivity, democracy, peace, the rule of law, sustainable development, and the enjoyment of human rights and fundamental freedoms. As we increasingly work, communicate, connect, engage, learn, and enjoy leisure time using digital technologies, our reliance on an open, free, global, interoperable, reliable, and secure Internet will continue to grow. Yet we are also aware of the risks inherent in that reliance and the challenges we face.

We call for a new Declaration for the Future of the Internet that includes all partners who actively support a future for the Internet that is an open, free, global, interoperable, reliable, and secure. We further affirm our commitment to protecting and respecting human rights online and across the digital ecosystem. Partners in this Declaration intend to work toward an environment that reinforces our democratic systems and promotes active participation of every citizen in democratic processes, secures and protects individuals' privacy, maintains secure and reliable connectivity, resists efforts to splinter the global Internet, and promotes a free and competitive global economy. Partners in this Declaration invite other partners who share this vision to join us in working together, with civil society and other stakeholders, to affirm guiding principles for our role in the future of the global Internet.

Reclaiming the Promise of the Internet

The immense promise that accompanied the development of the Internet stemmed from its design: it is an open "network of networks", a single interconnected communications system for all of humanity. The stable and secure operation of the Internet's unique identifier systems

have, from the beginning, been governed by a multi-stakeholder approach to avoid Internet fragmentation, which continues to be an essential part of our vision. For business, entrepreneurs, and the innovation ecosystem as a whole, interconnection promises better access to customers and fairer competition; for artists and creators, new audiences; for everyone, unfettered access to knowledge. With the creation of the Internet came a swell in innovation, vibrant communication, increased cross-border data flows, and market growth—as well as the invention of new digital products and services that now permeate every aspect of our daily lives.

Over the last two decades, however, we have witnessed serious challenges to this vision emerge. Access to the open Internet is limited by some authoritarian governments and online platforms and digital tools are increasingly used to repress freedom of expression and deny other human rights and fundamental freedoms. State-sponsored or condoned malicious behavior is on the rise, including the spread of disinformation and cybercrimes such as ransomware, affecting the security and the resilience of critical infrastructure while holding at risk vital public and private assets. At the same time, countries have erected firewalls and taken other technical measures, such as Internet shutdowns, to restrict access to journalism, information, and services, in ways that are contrary to international human rights commitments and obligations. Concerted or independent actions of some governments and private actors have sought to abuse the openness of Internet governance and related processes to advance a closed vision. Moreover, the once decentralized Internet economy has become highly concentrated and many people have legitimate concerns about their privacy and the quantity and security of personal data collected and stored online. Online platforms have enabled an increase in the spread of illegal or harmful content that can threaten the safety of individuals and contribute to radicalization and violence. Disinformation and foreign malign activity is used to sow division and conflict between individuals or groups in society, undermining respect for and protection of human rights and democratic institutions.

Our Vision

We believe we should meet these challenges by working towards a shared vision for the future of the Internet that recommits governments and relevant authorities to defending human rights and fostering equitable economic prosperity. We intend to ensure that the use of digital technologies reinforces, not weakens, democracy and respect for human rights; offers opportunities for innovation in the digital ecosystem, including businesses large and small; and, maintains connections between our societies. We intend to work together to protect and fortify

the multi-stakeholder system of Internet governance and to maintain a high level of security, privacy protection, stability and resilience of the technical infrastructure of the Internet.

We affirm our commitment to promote and sustain an Internet that: is an open, free, global, interoperable, reliable, and secure and to ensure that the Internet reinforces democratic principles and human rights and fundamental freedoms; offers opportunities for collaborative research and commerce; is developed, governed, and deployed in an inclusive way so that unserved and underserved communities, particularly those coming online for the first time, can navigate it safely and with personal data privacy and protections in place; and is governed by multi-stakeholder processes. In short, an Internet that can deliver on the promise of connecting humankind and helping societies and democracies to thrive.

The Internet should operate as a single, decentralized network of networks – with global reach and governed through the multi-stakeholder approach, whereby governments and relevant authorities partner with academics, civil society, the private sector, technical community and others. Digital technologies reliant on the Internet, will yield the greatest dividends when they operate as an open, free, global, interoperable, reliable, and secure systems. Digital technologies should be produced, used, and governed in ways that enable trustworthy, free, and fair commerce; avoid unfair discrimination between, and ensure effective choice for, individual users; foster fair competition and encourage innovation; promote and protect human rights; and, foster societies where:

Human rights and fundamental freedoms, and the well-being of all individuals are protected and promoted;

All can connect to the Internet, no matter where they are located, including through increased access, affordability, and digital skills;

Individuals and businesses can trust the safety and the confidentiality of the digital technologies they use

and that their privacy is protected;

• Businesses of all sizes can innovate, compete, and thrive on their merits in a fair and competitive ecosystem;

• Infrastructure is designed to be secure, interoperable, reliable, and sustainable;

• Technology is used to promote pluralism and freedom of expression, sustainability, inclusive economic growth, and the fight against global climate change.

Principles to promote this Vision

The partners in this Declaration intend to uphold a range of key principles, set out below, regarding the Internet and digital technologies; to promote these principles within existing multilateral and multi-stakeholder fora; to translate these principles into concrete policies and actions; and, work together to promote this vision globally, while respecting each other's regulatory autonomy within our own jurisdictions and in accordance with our respective domestic laws and international legal obligations. These principles are not legally binding but should rather be used as a reference for public policy makers, as well as citizens, businesses, and civil society organizations.

Protection of Human Rights and Fundamental Freedoms

Dedicate ourselves, in conducting and executing our respective domestic authorities, to respect human rights, including as reflected in the Universal Declaration of Human Rights, as well as the principles of the rule of law, legitimate purpose, non-arbitrariness, effective oversight, and transparency, both online and offline, and call upon others to do the same.

Promote online safety and continue to strengthen our work to combat violence online, including sexual and gender-based violence as well as child sexual exploitation, to make the Internet a safe and secure place for everyone, particularly women, children, and young people.

Promote safe and equitable use of the Internet for everyone, without discrimination based on sex, race, color, ethnic, national or social origin, genetic features, language, religion or belief, political or any other opinion, membership of an indigenous population, property, birth, disability, age, gender identity or sexual orientation.

Reaffirm our commitment that actions taken by governments, authorities, and digital services including online platforms to reduce illegal and harmful content and activities online be consistent with international human rights law, including the right to freedom of expression while encouraging diversity of opinion, and pluralism without fear of censorship, harassment, or intimidation.

Protect and respect human rights and fundamental freedoms across the digital ecosystem, while providing access to meaningful remedies for human rights violations and abuses, consistent with international human rights law.

Refrain from misusing or abusing the Internet or algorithmic tools or techniques for unlawful surveillance, oppression, and repression that do not align with international human rights principles, including developing social score cards or other mechanisms of domestic social control or pre-crime detention and arrest.

A Global Internet

Refrain from government-imposed internet shutdowns or degrading domestic Internet access, either entirely or partially.

Refrain from blocking or degrading access to lawful content, services, and applications on the Internet, consistent with principles of Net Neutrality subject to applicable law, including international human rights law.

Promote our work to realize the benefits of data free flows with trust based on our shared values as like-minded, democratic, open and outward looking partners.

Promote cooperation in research and innovation and standard setting, encourage information sharing regarding security threats through relevant international fora, and reaffirm our commitment to the framework of responsible state behavior in cyberspace.

Inclusive and Affordable Access to the Internet

Promote affordable, inclusive, and reliable access to the Internet for individuals and businesses where they need it and support efforts to close digital divides around the world to ensure all people of the world are able to benefit from the digital transformation.

Support digital literacy, skills acquisition, and development so that individuals can overcome the digital divide, participate in the Internet safely, and realize the economic and social potential of the digital economy.

Foster greater exposure to diverse cultural and multilingual content, information, and news online. Exposure to diverse content online should contribute to pluralistic public discourse, foster greater social and digital inclusion within society, bolster resilience to disinformation and misinformation, and increase participation in democratic processes.

Trust in the Digital Ecosystem

Work together to combat cybercrime, including cyber-enabled crime, and deter malicious cyber activity.

Ensure that government and relevant authorities' access to personal data is based in law and conducted in accordance with international human rights law.

Protect individuals' privacy, their personal data, the confidentiality of electronic communications and information on end-users' electronic devices, consistent with the protection of public safety and applicable domestic and international law.

Promote the protection of consumers, in particular vulnerable consumers, from online scams and other unfair practices online and from dangerous and unsafe products sold online.

Promote and use trustworthy network infrastructure and services suppliers, relying on risk-based assessments that include technical and

non-technical factors for network security.

Refrain from using the Internet to undermine the electoral infrastructure, elections and political processes, including through covert information manipulation campaigns.

• Support a rules-based global digital economy which fosters trade and contestable and fair online markets so that firms and entrepreneurs can compete on their merits.

• Cooperate to maximize the enabling effects of technology for combatting climate change and protecting the environment whilst reducing as much as possible the environmental footprint of the Internet and digital technologies.

Multi-stakeholder Internet Governance

Protect and strengthen the multi-stakeholder system of Internet governance, including the development, deployment, and management of its main technical protocols and other related standards and protocols.

Refrain from undermining the technical infrastructure essential to the general availability and integrity of the Internet.

We believe that the principles for the future of the Internet are universal in nature and as such we invite those who share this vision to affirm these principles and join us in the implementation of this vision. This Declaration takes into account, and expects to contribute to, existing processes in the UN system, G7, G20, the Organization for Economic Cooperation and Development, the World Trade Organization, and other relevant multilateral and multi-stakeholder fora, the Internet Corporation for Assigned Names and Numbers, Internet Governance Forum, and Freedom Online Coalition. We also welcome partnership with the many civil society organizations essential to promoting an open, free, global, interoperable, reliable, and secure Internet, and defending fundamental freedoms and human rights online. Partners in this Declaration intend to consult and work closely with stakeholders in carrying forward this vision. April, 2022

★ ★ ★ ★ ★

The 10 Biggest Revelations From Edward Snowden's Leaks

Secret court orders allow NSA to sweep up Americans' phone records

Verizon had been providing the NSA with virtually all of its customers' phone records. It soon was revealed that it was not just Verizon, but also virtually every other telephone company in America.

PRISM

Initially, reports described PRISM as the NSA's program to directly access the servers of U.S tech giants like Google, Facebook, Microsoft, and Apple, among others.

Britain's version of the NSA taps fiber optic cables around the world

The British spy agency, the Government Communications Headquarters (GCHQ), taps fiber optic cables all over the world to intercept data flowing through the global Internet, in a program that is codenamed Tempora.

NSA spies on foreign countries and world leaders

Over the months, countless stories based on Snowden documents have revealed that the NSA has spied on numerous world leaders and foreign governments.

XKeyscore, the program that sees everything

XKeyscore is a tool the NSA uses to search "nearly everything a user does on the Internet" through data, it intercepts across the world.

NSA efforts to crack encryption and undermine Internet security

Encryption makes data flowing through the Internet unreadable to hackers and spies, making the NSA's surveillance programs less useful. What is the point of tapping fiber optic cables if the data flowing through them is unreadable? That is why the NSA has a developed a series of techniques and tricks to circumvent widely used web encryption technologies.

NSA elite hacking team techniques revealed

The NSA has at its disposal an elite hacker team codenamed "Tailored Access Operations" (TAO) that hacks into computers worldwide, infects them with autonomous malware, and does the dirty job when other surveillance tactics fail.

NSA cracks Google and Yahoo data center links

When bulk collection or PRISM fails, the NSA had other tricks up its sleeve: It could infiltrate links connecting Yahoo and Google data centers, behind the companies' backs.

NSA collects text messages

It is not just about Internet data though. The NSA, following its unofficial motto of "collecting it all," intercepts 200 million text messages every day worldwide through a program called Dishfire.

10. NSA intercepts and stores all phone calls made in the Bahamas and Afghanistan through a program called MYSTIC.

8 Things That Happened Because Of The NSA Leaks

1. Director of National Intelligence James Clapper had to admit he lied to Congress. "I gave the least untruthful answer."

Three months before the Snowden leaks began; Sen. Ron Wyden (D-Ore.) asked the nation's top intelligence official if the NSA collected data on millions, or hundreds of millions, of Americans.

"No, sir," Clapper replied. "Not wittingly."

By that point, of course, the NSA had quite wittingly been running a massive bulk telephone metadata collection program for years. The government had repeatedly asked a secret surveillance court for permission to do so, and it deemed every American's phone record "relevant" to terrorism in the process.

Wyden fumed in secret about Clapper's lie — but felt he could not reveal it because the metadata collection program was classified. That all changed after the publication of the first story on June 5, 2013, based off a Snowden leak.

Days later, Clapper gave the most halfhearted, or perhaps least forthcoming, admission that he had lied: "I responded in what I thought was the most truthful or least untruthful manner by saying no."

2. The House passed a bill (ostensibly) meant to stop bulk collection of phone metadata.

Americans were furious about the NSA's sweeping phone metadata collection program. Even the man, who wrote the original Patriot Act, Wisconsin Republican Rep. James Sensenbrenner, said the program went too far.

So last month the House passed a bill that its sponsors said would end bulk collection. Whether it actually does is a matter of dispute, since the White House and the spy agencies appear to have stripped out many of its toughest provisions. But its passage is nonetheless a clear signal that nobody in Congress wants to look like they are doing nothing about the NSA.

3. A federal judge said the NSA phone surveillance program is unconstitutional.

In December, U.S. District Court Judge Richard Leon issued a ruling in a lawsuit against the NSA program that said its technology was "almost-Orwellian" and that James Madison "would be aghast."

Because other judges in other districts have found differently — one in Manhattan dismissed an American Civil Liberties Union lawsuit citing the threat of terrorists' "bold jujitsu" — the program still stands. And it had previously been approved, though behind closed doors, by the special Foreign Intelligence Surveillance Court. But with Leon's ruling on the books, the program could eventually wind up before the Supreme Court.

4. Tech companies finally got serious about privacy.

Big tech players had been paying lip service for years to the idea that they protect their customers' privacy. But after the Snowden revelation that the NSA was accessing company servers via its PRISM program, privacy suddenly became a very tangible good. Cloud providers stand to lose $35 billion over the next three years in business with foreign customers afraid of

storing their data with U.S. companies.

So the companies are responding by adding encryption measures such as Transport Layer Security. Google even announced on Tuesday that it is testing a new extension for the Chrome browser that could make encrypting email easier.

5. Britain held its first-ever open intelligence hearing.

If you thought intelligence oversight was weak in the United States, you will not believe how it works with our closest ally. The powerful British spy agencies MI5 and GCHQ had never faced a public hearing in front of Parliament until Snowden's stories dropped.

The November hearing was hardly confrontational. But it was a step forward for a country that has generally reacted to the Snowden leaks with little more than a shrug. And that step matters for Americans as well: In April, The Intercept revealed that the GCHQ had secretly asked for "unsupervised access" to the NSA's data pools.

6. Germany opened an investigation into the tapping of Chancellor Angela Merkel's cell phone.

The revelation that the NSA was monitoring the German chancellor's cell phone came as a surprise to her — and to Senate Intelligence Chairwoman Dianne Feinstein (D-Calif.). Merkel was so outraged that she reportedly compared the surveillance to that of the Stasi, the former East German spy agency. (And she would know, having grown up in East Germany.)

On Wednesday, German Federal Prosecutor Harald Range announced that he is opening an investigation into the monitoring of Merkel's phone calls. The investigation is proof positive that the Snowden leaks have frayed some U.S. diplomatic relations, but also that people the world over are starting to take surveillance seriously.

7. Brazil scotched a $4 billion defense contract with Boeing.

In another example of soured relations abroad, Brazil gave a massive fighter jet contract to Saab instead of the American company Boeing. Opinions varied as to how much that had to do with Snowden's leaks, with one government source telling Reuters that he "ruined it for the Americans." One analyst believed, however, that the Boeing jet simply cost too much.

The jet aside, Brazilian President Dilma Rousseff was clearly steamed, taking to the podium at the U.N. General Assembly to denounce the surveillance on her. Snowden's leaks also helped propel the passage of an Internet bill of rights meant to protect privacy in the South American nation.

8. President Barack Obama admitted there would be no surveillance debate without Snowden.

In a major speech in January, Obama said he was "not going to dwell on Mr. Snowden's actions or his motivations." But he essentially acknowledged that the roiling, yearlong debate over surveillance would not have happened without him.

"We have to make some important decisions about how to protect ourselves and sustain our leadership in the world, while upholding the civil liberties and privacy protections that our ideals — and our Constitution — require," Obama said.

The secretive Foreign Intelligence Surveillance Court also nodded

toward the "considerable public interest and debate" that Snowden's leaks created. And even Clapper acknowledged, "It's clear that some of the conversations this has generated, some of the debate, actually needed to happen."

The surveillance court finally started publicly posting some filings from its major cases. And in further acknowledgement of the need for a debate, the NSA and other agencies have posted declassified files to a new intelligence Tumblr — revealing for the first time aside from Snowden's leaks documentary evidence of the inner workings of mass surveillance.

By Matt Sledge HUFFPOST POLITICS 06/05/2014 07:31 am ET Updated Jun 05, 2014

Whistleblowing Is Not Just Leaking — It's an Act of Political Resistance

I've been waiting 40 years for someone like you." Those were the first words Daniel Ellsberg spoke to me when we met last year. Dan and I felt an immediate kinship; we both knew what it meant to risk so much — and to be irrevocably changed — by revealing secret truths.

One of the challenges of being a whistleblower is living with the knowledge that people continue to sit, just as you did, at those desks, in that unit, throughout the agency, who see what you saw and comply in silence, without resistance or complaint. They learn to live not just with untruths but also with unnecessary untruths, dangerous untruths, and corrosive untruths. It is a double tragedy: What begins as a survival strategy ends with the compromise of the human being it sought to preserve and the diminishing of the democracy meant to justify the sacrifice.

But unlike Dan Ellsberg, I did not have to wait 40 years to witness other citizens breaking that silence with documents. Ellsberg gave the Pentagon Papers to the New York Times and other newspapers in 1971; Chelsea Manning provided the Iraq and Afghan War logs and the Cablegate materials to WikiLeaks in 2010. I came forward in 2013. Now here we are in 2016, and another person of courage and conscience has made available the set of extraordinary documents that are published in The Assassination Complex, the new book out today by Jeremy Scahill and the staff of The Intercept. (The documents were originally published last October 15 in The Drone Papers.)

We are witnessing a compression of the working period in which bad policy shelters in the shadows, the time frame in which unconstitutional activities can continue before they are exposed by acts of conscience. And this temporal compression has a significance beyond the immediate headlines; it permits the people of this country to learn about critical government actions, not as part of the historical record but in a way that allows direct action through voting — in other words, in a way that empowers an informed citizenry to defend the democracy that "state secrets" are nominally intended to support. When I see individuals who are able to bring information forward, it gives me hope that we will not always be required to curtail the illegal activities of our government as if it were a constant task, to uproot official lawbreaking as routinely as we mow the grass. (Interestingly enough, that is how some have begun to describe remote killing operations, as "cutting the grass.")

A single act of whistleblowing does not change the reality that there are significant portions of the government that operate below the waterline, beneath the visibility of the public. Those secret activities will

continue, despite reforms. But those who perform these actions now have to live with the fear that if they engage in activities contrary to the spirit of society — if even a single citizen is catalyzed to halt the machinery of that injustice — they might still be held to account. The thread by which good governance hangs is this equality before the law, for the only fear of the man who turns the gears is that he may find himself upon them.

Hope lies beyond, when we move from extraordinary acts of revelation to a collective culture of accountability within the intelligence community. Here we will have taken a meaningful step toward solving a problem that has existed for as long as our government.

Not all leaks are alike, nor are their makers. Gen. David Petraeus, for instance, provided his illicit lover and favorable biographer information so secret it defied classification, including the names of covert operatives and the president's private thoughts on matters of strategic concern. Petraeus was not charged with a felony, as the Justice Department had initially recommended, but was instead permitted to plead guilty to a misdemeanor. Had an enlisted soldier of modest rank pulled out a stack of highly classified notebooks and handed them to his girlfriend to secure so much as a smile, he would be looking at many decades in prison, not a pile of character references from a Who's Who of the Deep State.

There are authorized leaks and also permitted disclosures. It is rare for senior administration officials to explicitly ask a subordinate to leak a CIA officer's name to retaliate against her husband, as appears to have been the case with Valerie Plame. It is equally rare for a month to go by in which some senior official does not disclose some protected information that is beneficial to the political efforts of the parties but clearly "damaging to national security" under the definitions of our law.

This dynamic can be seen quite clearly in the al Qaeda "conference call of doom" story, in which intelligence officials, likely seeking to inflate the threat of terrorism and deflect criticism of mass surveillance, revealed to a neoconservative website extraordinarily detailed accounts of specific communications they had intercepted, including locations of the participating parties and the precise contents of the discussions. If the officials' claims were to be believed, they irrevocably burned an extraordinary means of learning the precise plans and intentions of terrorist leadership for the sake of a short-lived political advantage in a news cycle. Not a single person seems to have been so much as disciplined as a result of the story that cost us the ability to listen to the alleged al Qaeda hotline.

If harmfulness and authorization make no difference, what explains the distinction between the permissible and the impermissible disclosure?

The answer is control. A leak is acceptable if it is not seen as a threat, as a challenge to the prerogatives of the institution. But if all of the disparate components of the institution — not just its head but its hands and feet, every part of its body — must be assumed to have the same power to discuss matters of concern, that is an existential threat to the modern political monopoly of information control, particularly if we're talking about disclosures of serious wrongdoing, fraudulent activity, unlawful activities. If you can't guarantee that you alone can exploit the flow of controlled information, then the aggregation of all the world's unmentionables — including your own — begins to look more like a liability than an asset.

Truly unauthorized disclosures are necessarily an act of resistance — that is, if they are not done simply for press consumption, to fluff up the public appearance or reputation of an institution. However, that does not mean they all come from the lowest working level. Sometimes the individuals who step forward happen to be near the pinnacle of power. Ellsberg was in the top tier; he was briefing the secretary of defense. You cannot get much higher, unless you are the secretary of defense, and the incentives simply are not there for such a high-ranking official to be involved in public interest disclosures because that person already wields the influence to change the policy directly.

At the other end of the spectrum is Manning, a junior enlisted soldier, who was much nearer to the bottom of the hierarchy. I was midway in the professional career path. I sat down at the table with the chief information officer of the CIA, and I was briefing him and his chief technology officer when they were publicly making statements like "We try to collect everything and hang on to it forever," and everybody still thought that was a cute business slogan. Meanwhile I was designing the systems they would use to do precisely that. I was not briefing the policy side, the secretary of defense, but I was briefing the operations side, the National Security Agency's director of technology. Official wrongdoing can catalyze all levels of insiders to reveal information, even at great risk to themselves, so long as they can be convinced that it is necessary to do so.

Reaching those individuals, helping them realize that their first allegiance as a public servant is to the public rather than to the government, is the challenge. That is a significant shift in cultural thinking for a government worker today.

I have argued that whistleblowers are elected by circumstance. It is not a virtue of who you are or your background. It is a question of what you are exposed to, what you witness. At that point the question becomes do you honestly believe that you have the capability to remediate the problem, to influence policy? I would not encourage individuals to reveal

information, even about wrongdoing, if they do not believe they can be effective in doing so, because the right moment can be as rare as the will to act.

This is simply a pragmatic, strategic consideration. Whistleblowers are outliers of probability, and if they are to be effective as a political force, it is critical that they maximize the amount of public good produced from scarce seed. When I was making my decision, I came to understand how one strategic consideration, such as waiting until the month before a domestic election, could become overwhelmed by another, such as the moral imperative to provide an opportunity to arrest a global trend that had already gone too far. I was focused on what I saw and on my sense of overwhelming disenfranchisement that the government, in which I had believed for my entire life, was engaged in such an extraordinary act of deception.

Change has to flow from the bottom to the top.

At the heart of this evolution is that whistleblowing is a radicalizing event — and by "radical" I don't mean "extreme"; I mean it in the traditional sense of radix, the root of the issue. At some point, you recognize that you cannot just move a few letters around on a page and hope for the best. You cannot simply report this problem to your supervisor, as I tried to do, because inevitably supervisors get nervous. They think about the structural risk to their career. They are concerned about rocking the boat and "getting a reputation." The incentives are not there to produce meaningful reform. Fundamentally, in an open society, change has to flow from the bottom to the top.

As someone who works in the intelligence community, you have given up a lot to do this work. You have happily committed yourself to tyrannical restrictions. You voluntarily undergo polygraphs; you tell the government everything about your life. You waive a lot of rights because you believe the fundamental goodness of your mission justifies the sacrifice of even the sacred. It is a just cause.

And when you are confronted with evidence — not in an edge case, not in a peculiarity, but as a core consequence of the program — that the government is subverting the Constitution and violating the ideals, you so fervently believe in, you have to make a decision. When you see that the program or policy is inconsistent with the oaths and obligations that you have sworn to your society and yourself, then that oath and that obligation cannot be reconciled with the program. To which do you owe a greater loyalty?

One of the extraordinary things about the revelations of the past several years, and their accelerating pace, is that they have occurred in the context of the United States as the "uncontested hyperpower." We now have the largest unchallenged military machine in the history of the

world, and it is backed by a political system that is increasingly willing to authorize any use of force in response to practically any justification. In today's context, that justification is terrorism, but not necessarily, because our leaders are particularly concerned about terrorism in itself or because they think it is an existential threat to society. They recognize that even if we had a 9/11 attack every year, we would still be losing more people to car accidents and heart disease, and we do not see the same expenditure of resources to respond to those more significant threats.

What it really comes down to is the political reality that we have a political class that feels it must inoculate itself against allegations of weakness. Our politicians are more fearful of the politics of terrorism — of the charge that they do not take terrorism seriously — than they are of the crime itself.

As a result, we have arrived at this unmatched capability, unrestrained by policy. We have become reliant upon what was intended to be the limitation of last resort: the courts. Judges, realizing that their decisions are suddenly charged with much greater political importance and impact than was originally intended, have gone to great lengths in the post-9/11 period to avoid reviewing the laws or the operations of the executive in the national security context and setting restrictive precedents that, even if entirely proper, would impose limits on government for decades or more. That means the most powerful institution that humanity has ever witnessed has also become the least restrained. Yet that same institution was never designed to operate in such a manner, having instead been explicitly founded on the principle of checks and balances. Our founding impulse was to say, "Though we are mighty, we are voluntarily restrained."

When you first go on duty at CIA headquarters, you raise your hand and swear an oath — not to government, not to the agency, not to secrecy. You swear an oath to the Constitution. So there is this friction, this emerging contest between the obligations and values that the government asks you to uphold, and the actual activities that you are asked to participate in.

These disclosures about the Obama administration's killing program reveal that there is a part of the American character that is deeply concerned with the unrestrained, unchecked exercise of power. And there is no greater or clearer manifestation of unchecked power than assuming for oneself the authority to execute an individual outside of a battlefield context and without the involvement of any sort of judicial process.

Traditionally, in the context of military affairs, we have always understood that lethal force in battle could not be subjected to ex ante judicial constraints. When armies are shooting at each other, there is no room for a judge on that battlefield. But now the government has decided

— without the public's participation, without our knowledge and consent — that the battlefield is everywhere. Individuals who do not represent an imminent threat in any meaningful sense of those words are redefined, through the subversion of language, to meet that definition.

Inevitably, that conceptual subversion finds its way home, along with the technology that enables officials to promote comfortable illusions about surgical killing and nonintrusive surveillance. Take, for instance, the Holy Grail of drone persistence, a capability that the United States has been pursuing forever. The goal is to deploy solar-powered drones that can loiter in the air for weeks without coming down. Once you can do that, and you put any typical signals collection device on the bottom of it to monitor, unblinkingly, the emanations of, for example, the different network addresses of every laptop, smartphone, and iPod, you know not just where a particular device is in what city, but you know what apartment each device lives in, where it goes at any particular time, and by what route. Once you know the devices, you know their owners. When you start doing this over several cities, you are tracking the movements not just of individuals but also of whole populations.

Unrestrained power may be many things, but it is not American.

By preying on the modern necessity to stay connected, governments can reduce our dignity to something like that of tagged animals, the primary difference being that we paid for the tags and they are in our pockets. It sounds like fantasist paranoia, but on the technical level, it is so trivial to implement that I cannot imagine a future in which it will not be attempted. It will be limited to the war zones at first, in accordance with our customs, but surveillance technology has a tendency to follow us home.

Here we see the double edge of our uniquely American brand of nationalism. We are raised to be exceptionalists, to think we are the better nation with the manifest destiny to rule. The danger is that some people will actually believe this claim, and some of those will expect the manifestation of our national identity, that is, our government, to comport itself accordingly.

Unrestrained power may be many things, but it is not American. It is in this sense that the act of whistleblowing increasingly has become an act of political resistance. The whistleblower raises the alarm and lifts the lamp, inheriting the legacy of a line of Americans that begins with Paul Revere.

The individuals who make these disclosures feel so strongly, about what they have seen that they are willing to risk their lives and their freedom. They know that we, the people, are ultimately the strongest and most reliable check on the power of government. The insiders at the highest levels of government have extraordinary capability,

extraordinary resources, tremendous access to influence, and a monopoly on violence, but in the final calculus, there is but one figure that matters: the individual citizen.

And there are more of us than there are of them.

Edward Snowden May 3 2016, 5:00 a.m.